
# EMPOWERING MARINE CORPS SYSTEM ADMINSTRATORS:

# TAXONOMY OF TRAINING

THESIS

Brian K. Hamilton, GySgt, USMC

AFIT/GIR/ENV/04M-09

**DEPARTMENT OF THE AIR FORCE**

**AIR UNIVERSITY**

***AIR FORCE INSTITUTE OF TECHNOLOGY***

**Wright-Patterson Air Force Base, Ohio**

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, United States Marine Corps, Department of the Navy, or the United States Government.

AFIT/GIR/ENV/04M-09

# EMPOWERING MARINE CORPS SYSTEM ADMINSTRATORS:

# TAXONOMY OF TRAINING

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Brian K. Hamilton, BS

GySgt, USMC

March 2004

AFIT/GIR/ENV/04M-09

# EMPOWERING MARINE CORPS SYSTEM ADMINSTRATORS:

# TAXONOMY OF TRAINING

Brian K. Hamilton, BS

GySgt, USMC

Approved:

| | |
|---|---|
| //SIGNED// | 25 MAR 04 |
| Alan R. Heminger, PhD (Chairman) | date |
| //SIGNED// | 25 MAR 04 |
| Kevin L. Elder, PhD (Member) | date |
| //SIGNED// | 25 MAR 04 |
| Edward D. White III, PhD (Member) | date |

AFIT/GIR/ENV/04M-09


## Abstract

Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that System Administrators are properly trained and meet a minimum standard that is enforced enterprise-wide. Only with this ubiquitous benchmark training, will the System Administrators roles and responsibilities become synchronous to achieving Defense in Depth in the IT realm. The goal of this research is to analyze Marine Corps training methods to identify viable solutions that will produce consistent skill sets and meet requirements set forth in mandates from DoD.

## Acknowledgements

Thank you to my fellow students for their support throughout this graduate study, particularly Juan & Kelvin & Jim, who studied along side me, long into the night.

Thank you to my committee members, all of whom are current or adjunct instructors at the Air Force Institute of Technology: Doctor Alan Heminger, my advisor, and Doctor Kevin Elder and Doctor Tony White, my readers. I was by no means your best student, but I certainly learned a lot from you over the last eighteen months.

Thank You to LtCol Bartczak and LtCol Swartz. Both of these Officers were very inspirational throughout my tenure here. I will apply the lessons that they have taught me for years to come.

This has been a challenging learning and growth experience on academic, professional, and personal level for me. I am extremely grateful for it, and I hope to make the most of what I have learned throughout the rest of my life.

Thank you to my wife and best friend, for her tireless encouragement, support, and understanding throughout. No words here could capture what she means to me, or how she has inspired me during this process and throughout my daily life.

## Table of Contents

Page

## List of Figures

## List of Tables

EMPOWERING MARINE CORPS SYSTEM ADMINISTRATORS:

TAXONOMY OF TRAINING

# I. Introduction

## 1.1 General Issue

The Chairman of the Joint Chiefs of Staff has mandated that all System Administrators (SA), be certified and cleared to the level of information classification for a given system. This mandate applies equally to uniformed Service members, Department of Defense (DOD) civilians, and contract personnel. This also includes part-time or collateral-duty SA. The training to comply with this mandate does not need to award military specialty or training codes but must meet criteria set forth in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01.

Network or computer systems administrators design, install, and support an organization's LAN, WAN, network segment, Internet, or Intranet system. They provide day-to-day onsite administrative support for software users in a variety of work environments, including offices, warehouses, deployed environments and on-board ship. They maintain network hardware and software, analyze problems, and monitor the network to ensure availability to system users. These workers gather data to identify customer needs and then use that information to identify, interpret, and evaluate system and network requirements. Administrators also may plan, coordinate, and implement network security measures.

Systems administrators are the information technology Marines responsible for the efficient use of networks by organizations. They ensure that the design of an

organization's computer site allows all the components, including computers, the network, and software, to fit together and work properly. Furthermore, they monitor and adjust performance of existing networks and continually survey the current computer site to determine future network needs. Administrators also troubleshoot problems as reported by users and automated network monitoring systems and make recommendations for enhancements in the construction of future servers and networks. (Dept of Labor, 2003)

### 1.2 Network-Centric Fighting Force

Currently the mandate set forth in CJCSM 6510.01 is being met Marine Corps wide, by personnel specifically assigned by military occupational specialty (MOS), by military personnel who have dual roles and responsibilities and civilian General Schedule (GS) workers. Contractors also make up a small amount of the Corps wide System Administrators.

The human factor is so critical to success that the Computer Security Act of 1987 (Public Law [P.L.] 100-235) required that, "*Each agency shall provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency.*" (NIST 800-16, 1998)

The Marine Corps has become a Network-Centric fighting force with increasing reliance on the information systems that hold the key data for command and control. As this ubiquitous computing has reached into the depths of almost all units

within the Marine Corps, it is imperative that, as the technology expands, training of the System Administrators will also expand.

In today's Marine Corps, information systems not only support command and control functions but are also an integral part of business operations. For example, the Asset Tracking Logistics and Supply System (ATLASS II+) is a deployable supply, maintenance, and material readiness automated system. It is compliant with the Defense Information Infrastructure Common Operating Environment (DII COE) in order to provide asset visibility and logistics posture to higher, adjacent, and supporting units thus providing greater situational awareness on the battlefield.

This system is now essential for units and their supply chains. Incorrect information in an ATLASS II+ system can have mission-critical consequences for the logistic supply chain of the units, whether they are garrison based or deployed.

In November of 2002, Headquarters Marine Corps (HQMC) published Marine Corps Order MCO 5239.2, which implemented an Information Assurance (IA) Policy throughout the Marine Corps. This IA policy set forth procedures for all Information Technology (IT) resources procured, developed, operated, maintained, or managed throughout the Marine Corps. One of the concepts of operations specified in this policy was that System Administrators receive detailed training relative to their duties.

In March of 2003, the Chairman of the Joint Chiefs of Staff published that mandated SA be certified via certification requirements for Department of Defense (DOD) systems. The manual also dictates that there will be three levels of System Administrators, novice, intermediate and advanced. These SA levels are in conjunction

with experience levels, respectively, less then three years, three to five years and five years and beyond respectively.

For many years system administration has been passed on to new generations through manual pages, technical handbooks and by word of mouth. In all but the most disciplined institutions this has been a haphazard affair with a disregard for theory and no common standard of practice. In recent years, the arrival of the Internet has made this untenable. The level of complexity of networked operating systems together with the increasing problem of intrusion (`cracking') has now elevated system administration to a discipline in its own right. (Brenner 2001)

### 1.3 Problem Statement

The specific problem for this research effort is to determine if the Marine Corps's existing system administrator training meets requirements mandated by current DOD publications. Included in the research will be an assessment of alternative training methods such as On the Job Training (OJT), which can be used to meet the criteria set forth in the CJCSM 6510.01.

### 1.4 Research Objectives & Investigative Questions

The objective of this research is twofold. The first is to document the current methods employed by the Marine Corps for the training of System Administrators. Second, to document the mandated requirements for Level One System Administrators from the CJCSM 6510.01, The National Institute of Standards and Technology, (NIST) Special Publication 800-16, and the National Security Telecommunications and Information Systems Security Committee, (NSTISSI) Publication Number 4013.

By developing a taxonomy between current training, and SA Level One skill sets, this research will identify any key enablers or gaps that exist. By examining existing training, it is the goal of this research to identify DOD promulgated requirements and compare these with the current training of Marine Corps System Administrators.

The investigative questions that will be addressed in this research effort are as follows:

1. Where is the training being conducted for the 06XX Occupational Field that meets the requirements mandated by CJCSM to certify Marine Corps System Administrators at the novice level?
2. Are private industry certifications an alternative method that can be used for DoD System Administrator certification?
3. Is there a correlation between the quality of training and the delivery method?

**1.5 Scope of the Study**

This thesis is a follow on study to the previous research done by the Defense Information Assurance Program (DIAP). The DIAP research identified various sources of certification.

The scope of this research will focus on:

- The Marine Corps population of SAs.
- SA Level Ones

### 1.6 Proposed Methodology

The data will be collected via surveys, from System Administrators throughout the Marine Corps. With the implementation of the Navy Marine Corps Intranet (NMCI), it is imperative that System Administrators from within and outside the NMCI realm be surveyed.

Once it all the data is collected, it will be compiled, correlated, content reviewed for application to this study. The data form will be comprised of survey results.

The methodology used will be a combination of the literature review, surveys, structured and unstructured interviews and E-mails. Once this initial data is compiled and interpreted, an iterative survey will be sent to a sample of the SA population within the Marine Corps.

# II. Literature Review

## 2.1 Focus of Literature Review

This literature review discusses the body of research devoted to information assurance (IA) practices across DOD. By exploring, defining and detailing IA, this will provide a benchmark for the further exploration of SA training and certification.

The first section of this review introduces the background and history of information assurance and information assurance within the DoD. Next, is a brief review of threats and trends that are rampant throughout the networked world to include a quick look at the Computer Security Institute Crime Survey. Following this is an examination of the existing structure of the Marine Corps computer MOS's and their relative responsibilities. Finally is a review on the strategies used by the DoD to map specific requirements to Knowledge, Skills and Abilities. (KSA's).

## 2.2 Information Assurance Background

Information Assurance is defined in the CJCSM 6510.01 as "*Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection and reaction capabilities*." (CJCSM 2003)

Complete confidence in the trustworthiness of IT, users and interconnections cannot be achieved; therefore the DoD must embrace a risk management approach that balances the importance of the information and supporting technology to DoD missions against documented threats and vulnerabilities, the trustworthiness of users and interconnecting systems, and the effectiveness of IA solutions. (DODI 8500.2, 2003)

IA is an offshoot of the Defense in Depth concept. The Defense in Depth approach builds mutually supporting layers of defense to reduce vulnerabilities and to assist us to protect against, detect, and react to as many attacks as possible. By constructing mutually supporting layers of defense, this will cause an adversary who penetrates or breaks down one defensive layer to promptly encounter another, and another, until unsuccessful in the quest for unauthorized entrance, the attack ends. To protect against different attack methods, corresponding security measures must be employed. The weakness of one security measure should be compensated for by the strength of another. (DISA 2001).

The IA Defense in Depth (DiD) strategy is central to the objectives of JV 2020, which is aimed toward improving the processes and capabilities that the military needs to succeed in what will be the ever more complex global environment of the year 2020.

The ultimate goal of JV 2020 is Full Spectrum Dominance, which relies on dominant maneuvers, precision engagements, focused logistics, and full-dimensional protection. Full Spectrum Dominance relies on the concepts of Information Superiority and Innovation, each with IA at its core. (DoD CIO 2000).

The Defense in Depth interpretation is to not count on any single type of protection for information systems, but to instead provide levels of protection upon

protection. The analogy of this concept is the medieval castle that had the moat, the drawbridge, outer castle walls, inner castle walls and the keep. No single form of defense is foolproof, thus each layer compensates for deficiencies in the other layers. One of the key enablers of this Defense in Depth concept is properly trained System administrators.

System administrators are the individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information policy and procedures. (CJCSM 6510.01)

### 2.3 System Administrators within the DoD

Training personnel and organizations responsible for planning and conducting Information Assurance on all available capabilities will contribute significantly to successful offensive and defensive Information Operations (IO). Typically, the DoD has placed an individual to manage the systems in addition to their regular tasks.

Within the past ten years, the internet has evolved into a critical component of the DoD business infrastructure. This evolution has in turn driven the IT profession. As computers became more and more intrinsic to the unit's mission, computers and networking became an issue. Individuals would often be assigned to manage the systems in addition to their regular tasks. Usually this position would fall to the most technically-able body available. Most systems administrators are not recognized as such by their job titles. In their 1999 salary studies, the Systems Administrators' Guild (SAGE) reported that fewer than half of all people actually doing systems administration are employed by that title. (SAGE 2001).

## 2.4 Role & Responsibilities of DoD System Administrators

A SA is defined as: Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established information security policy and procedures. (NSTISSI 4009, 2001)

CJCSM 6510.01 mandates that System Administrators will be responsible for the following responsibilities:

(1) Maintain information system and networks, to include hardware and software.

(2) Monitor information system performance and system recovery processes to ensure security features and procedures are properly restored.

(3) Work closely with the IAO to ensure the information system or network is used and administered securely.

(4) Participate in the incident reporting program and conduct reporting in accordance with this manual.

(5) Provide customer support and ensure that all users have the requisite security clearances, authorization, need to know, and are aware of their security responsibilities before granting access to the information system.

(6) Assist the IAO in ensuring the system is operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the accreditation and certification support documentation package.

(7) Confirm software licenses and documentation are maintained by the

configuration management office, and notify the IAM and IAO when changes occur that might affect accreditation and certification.

(8) In coordination with CM office, ensure CM for security-relevant information system software and hardware, to include information system warning banners, is maintained and documented. Apply appropriate security technical implementation guides (STIGs) and periodically re-verify compliance.

(9) Assist IAM and IAO in development and maintenance of accreditation and certification support documentation package.

(10) Establish audit trails (system logs) and conduct reviews periodically (weekly or daily), and ensure audit records are archived for future reference as directed by the IAO and IAM.

(11) Provide backup of system operations.

(12) Conduct periodic reviews to ensure compliance with the accreditation and certification support documentation package.

(13) Respond to IAVAs, information assurance vulnerability bulletins (IAVBs), and other vulnerability notifications by obtaining and installing system patches, making procedural changes, and reporting IAVA compliance to the appropriate authority.

(14) In coordination with CM office, maintain and document the CM of the information system to include software, hardware, and warning banners. Assist the IAO in maintaining configuration control of the systems and applications software.

(15) Advise the IAO of security anomalies or integrity loopholes.

(16) In coordination with the IAO, administer user identification and authentication mechanism(s) of the information system or network.

(17) Attend required technical (e.g., operating system, networking, or system administration) and security (e.g., security management) training relative to assigned duties. (CJCSM 6510.01)

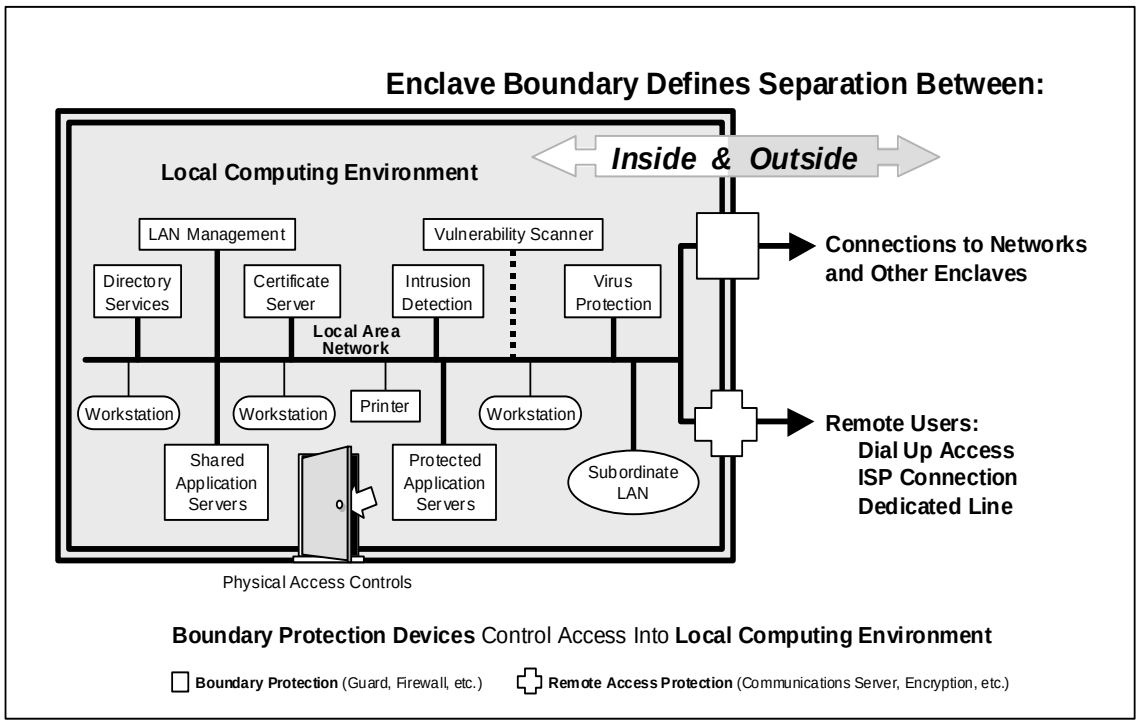



**Figure 1: Defending the Enclave Boundary (CJCSM 2003)**

As Figure 1 illustrates, System Administrators have to be well versed in numerous areas for them to be effective at their job.

## 2.5 System Administrator Knowledge Management

Within DoD, SAs are the people responsible for the defense of the cyber structure. Their job is to ensure organizations' systems are functioning properly while secure from various threats. Because even a single vulnerability in a computer or network setup can provide a means of unauthorized access, systems administrators must have adequate technical and managerial skills to ensure security. A properly trained and experienced systems staff is essential to the security of an organization's computer network. What SAs know, how they come to know it, and how they augment their knowledge are key areas that continue to be studied in the field. (Hrebec 2001)

Questions about SAs levels of experience and training are constant:

- What is the depth of the SAs understanding?
- What is the importance of formal training?
- What is the significance of understanding hardware?
- What are the abilities of the SA to handle novel problems?
- How are novel problems handled?
- Does the SA know the differences in different operating systems?
- Are the SAs receiving the support they require?

(Hrebec 2001)

## 2.6 Information Assurance vs. Network Security

It is important to note that within the realm of IT, there is a fine line between the definitions of network security and information assurance. Bellocci et al. define information assurance as a combination of:

1) Information security

2) Information integrity

3) Information significance

*Information security* means protecting information from malicious threats and damage due to external or internal sources. *Information integrity* should be understood as permanency of the information during communications and storage.
Lastly, *information significance* refers to the value that the intended user can get out of the information when they receive it. (Bellocci et al 2001)

Following this example, it is determined for this research effort that information assurance combines the requirements of information security, integrity and significance.

To further the discussion of the overlapping responsibilities of a network security specialist and a system administrator the Federal Enterprise Architecture Framework (FEAF) presents four separately defined but interrelated architectural layers, depicted in Figure 2.

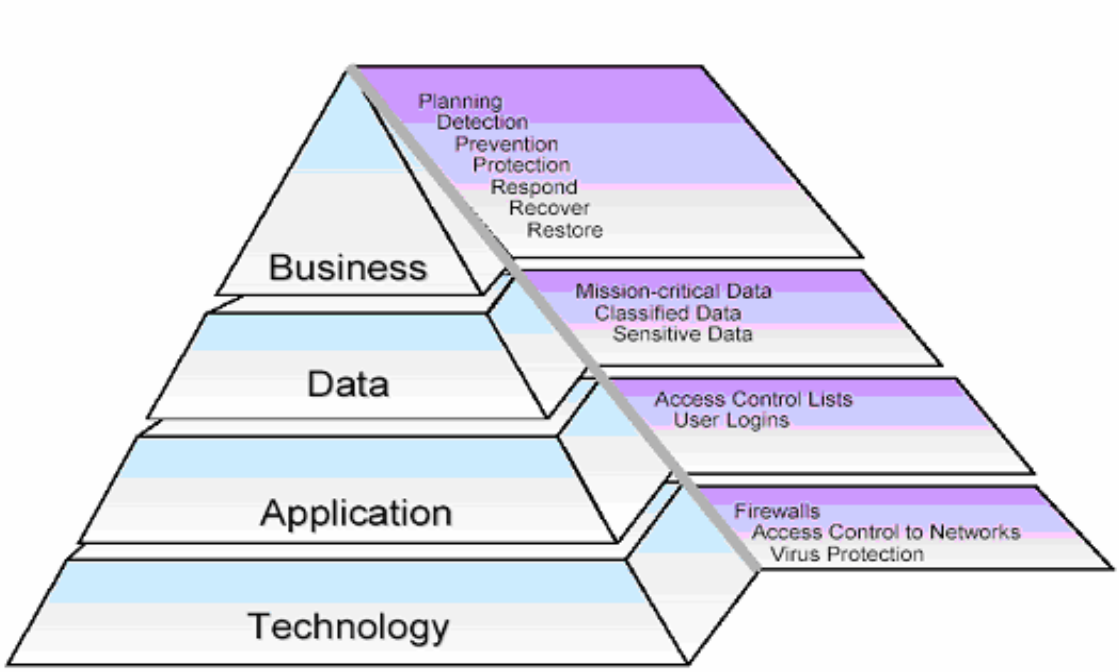



**Figure 2: Federal Enterprise Architecture Framework (Fed CIO, 1998)**

The layers are defined as follows:

*Business architecture*, which defines the business processes needed to per-form the business functions that the organization undertakes to achieve its goals and thereby accomplish its mission. It also addresses the sequence in which the business processes occur. This layer assists in defining mission-critical functions, identifying the personnel performing those functions, and identifying the locations where the functions are performed. *Data architecture*, which defines the pieces of information and their inter-relationships. This layer assists in identifying the data required by the organization to fulfill its mission-critical functions.

*Application architecture*, which defines the applications needed to manage data and support business functions. This layer also assists in identifying the personnel who have access to those applications.

*Technology architecture*, which describes the hardware and systems soft-ware, including operating systems and middleware. This layer assists in defining the infrastructure needed to perform the mission-critical functions.

### 2.7 DoD Information Assurance

One of the major challenges in ensuring information assurance is to understand the pervasiveness impact of information assurance across the enterprise. The DoD has taken a enterprise architecture approach to addressing information assurance because it ensures a structured and comprehensive process for evaluating the impact and consequences of changes in the functional environment (business processes, personnel, organizational units, locations) and the technical environment (data, applications, and technology used to support the business environment).

Information Assurance is not a new concept nor is the requirements to fulfill the IA concept. In 1997, the Assistant Secretary of Defense stated the need for DOD IA personnel to be identified, training verified, have an established career track and provided with opportunities to further enhance their skills.

Recently, the President's Critical Infrastructure Protection Board (PCIPB) established a committee on education. This committee is charged with developing policy and programs for training IT security personnel for the federal government and private enterprise.

Information assurance is more than a simple set of rules or procedures; it is an integral part of the Marine Corps' network centric environment. It is no longer just the network security personnel that is responsible for the integrity of the enterprise, the responsibility resides with all members of an organization.

A continuum of this concept is the education and training levels of key personnel. The diagram below illustrates how education is an integral part of information assurance process. "Awareness" constitutes the point-of-entry for all employees into the progression of IT security knowledge levels; the "Training" level, starting with "Security Basics and Literacy," then builds a wide range of security-related skills needed by employees in several functional area categories; and the "Education" level is the capstone of the learning continuum—creating expertise necessary for IT security specialists and professionals. (Maconachy 1988)

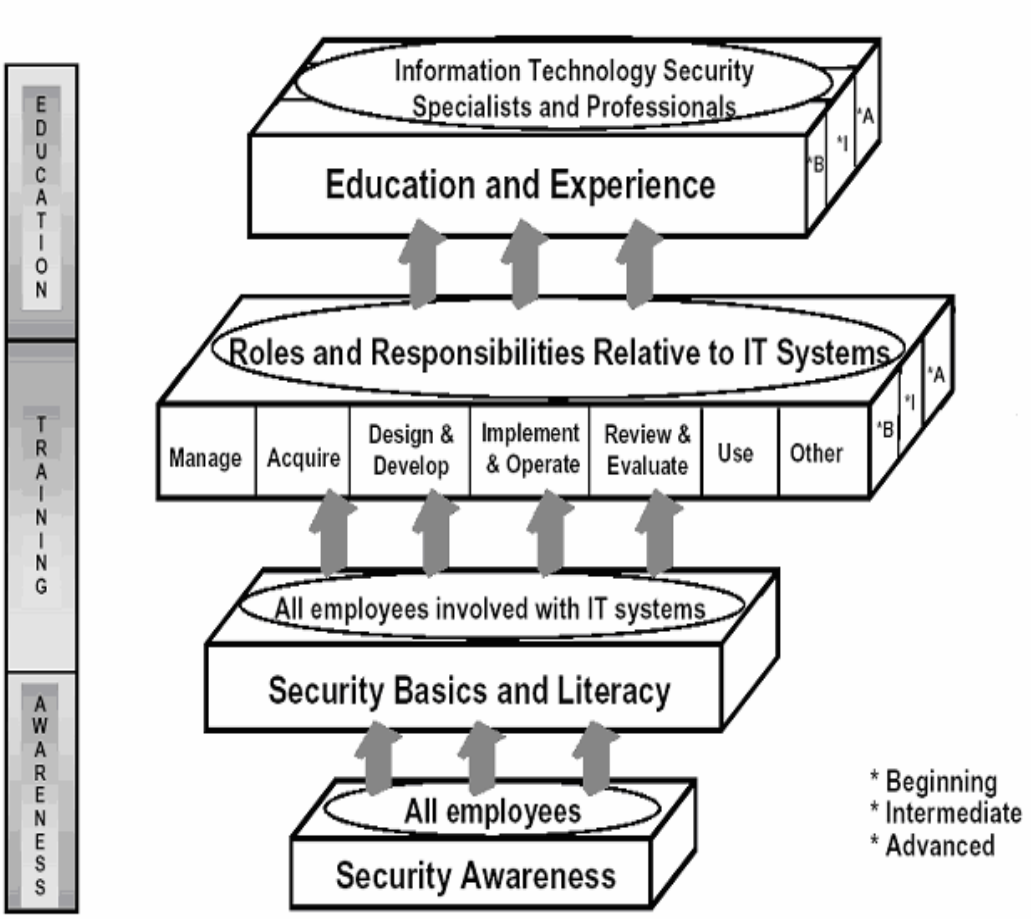



**Figure 3: IT Security Learning Continuum (NIST 800-16, 1998)**

## 2.8 Attacks, Social Engineering & Online Users

The threat from computer crime and information security breeches has continually climbed exponentially within the last five years. Targeted are the components of the information and economic infrastructures. DoD systems have continually been under attack for the last decade. These incidents are a common occurrence and widespread.

Hacking the computer systems is not the only approach that is used to violate networks. Social Engineering was brought to the spotlight by Kevin Mitnick, the first person to ever be convicted and jailed for hacking someone else's computer. "People are

the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything." (Smith 2001)

Social Engineering is defined by Professor Susan Brenner of the University Of Dayton School Of Law as a term used among hackers for cracking techniques that rely on weaknesses in people rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security. Classic scams include phoning up a mark that has the required information and posing as a field service tech or a fellow employee with an urgent access problem. (Brenner, 2001)

The art of estimating how many are online throughout the world is an inexact one at best. An educated guess is as of September 2002, there were 605.60 million users online, worldwide. In April of 1995 there were 18 million US users online, which represented 6.7 % of the population. In April of 2002, there were 165.75 million US users online, representing 59.1% of the US population. This is a 52.4% increase of the amount of US users online within a seven year period. (NAU 2002)

### 2.9 Computer Crime Survey

The definitive Crime and Security Survey published by Computer Security Institute has been tracking attacks and intrusions over the last seven years. The results of this survey are published on an annual basis and highlight the burgeoning problem of keeping networks secure across corporate America. As shown in the graph below, The Federal Government is not immune to attacks. Seven percent of the responses were from the Federal Government. (CSI/FBI 2003)

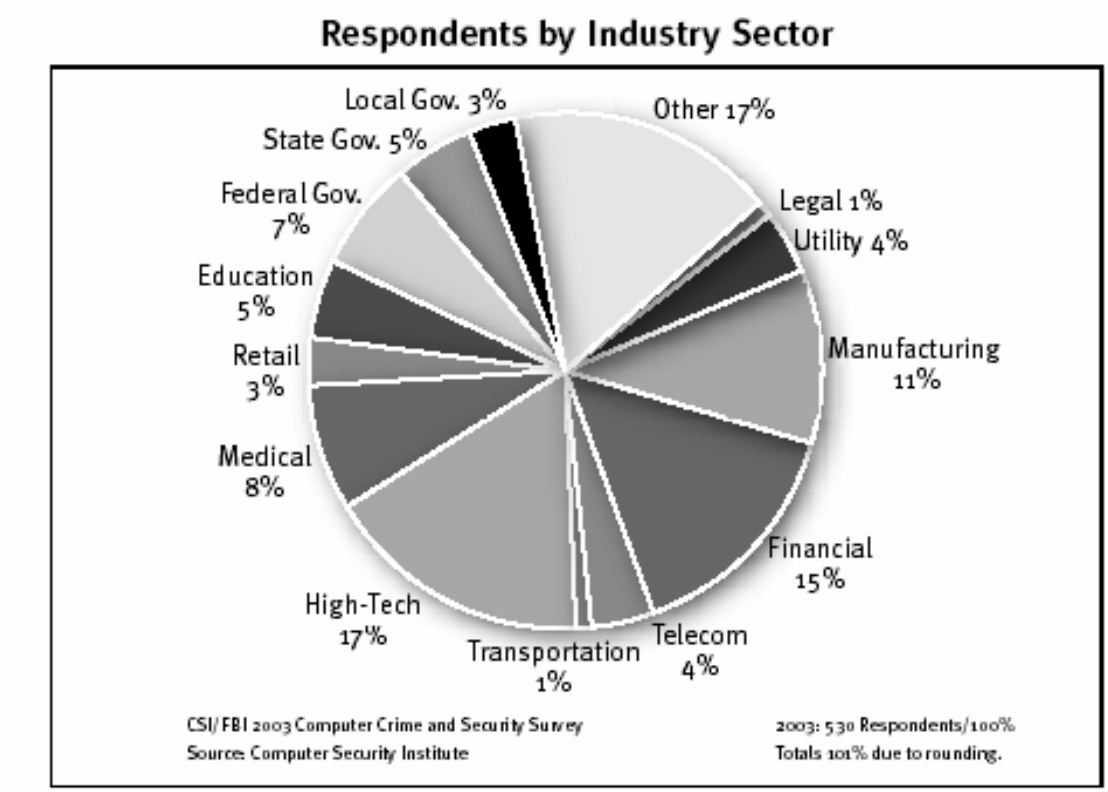



**Figure 4: Respondents of CSI/FBI Survey (CSI/FBI, 2003)**

Although unauthorized use of computer systems is still a concern, the graph below highlights the growing security trends that have been enacted to counter the unauthorized uses of computer systems over the last five years. These are the security trends that System Administrators have to be knowledgeable in to counteract the constant threat of attack.

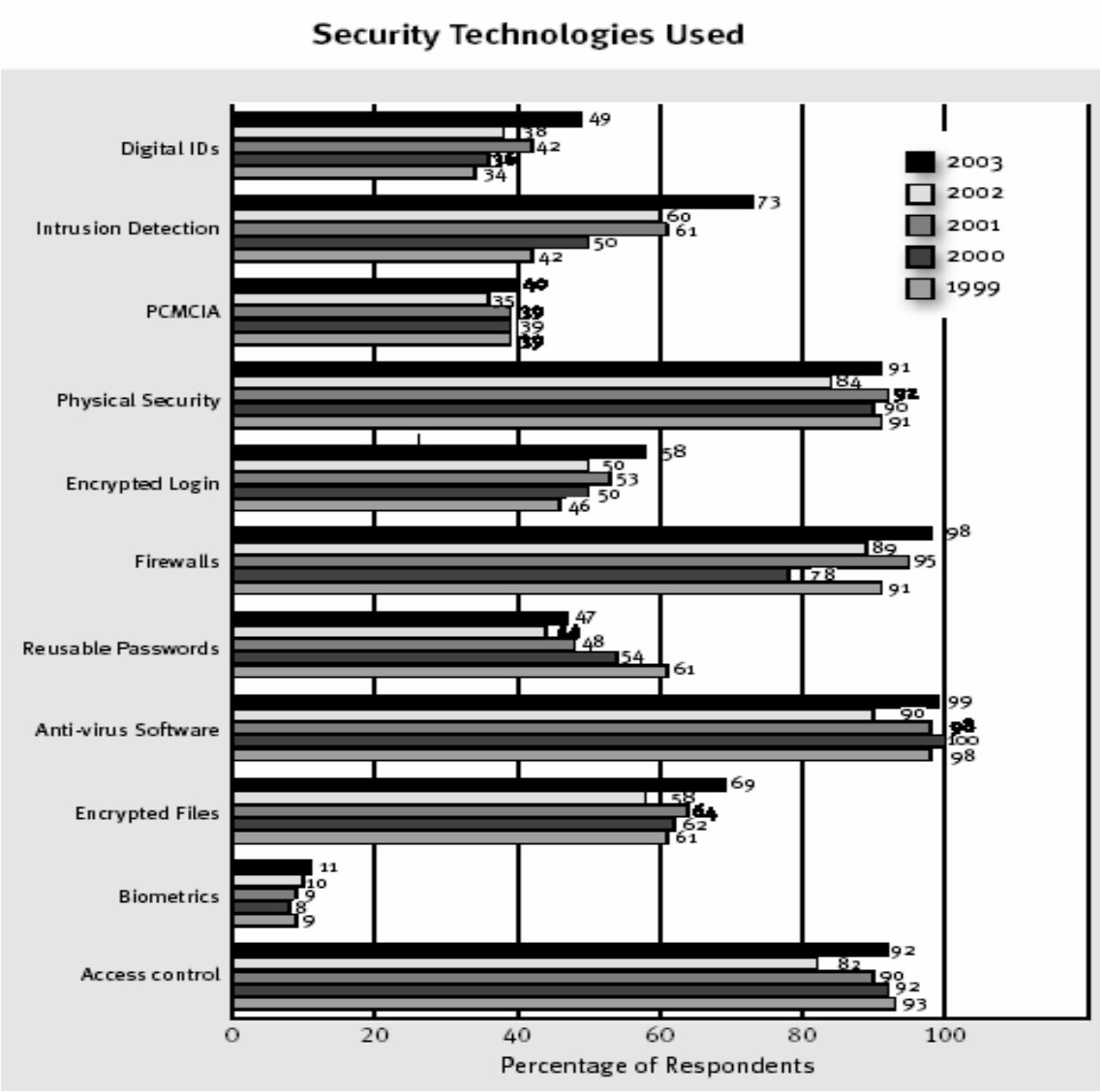



**Figure 5: Security Technologies Used (CSI/FBI 2003)**

Information assurance is a means to protect and defend DoD systems in the "arms race" against would be hackers. In 2003, sabotage of the networks has accounted for over 5 million dollars in lost revenue in the last 12 months and these figures only represent businesses that responded to the CSI/FBI survey.

## 2.10 System Administrators within the Marine Corps

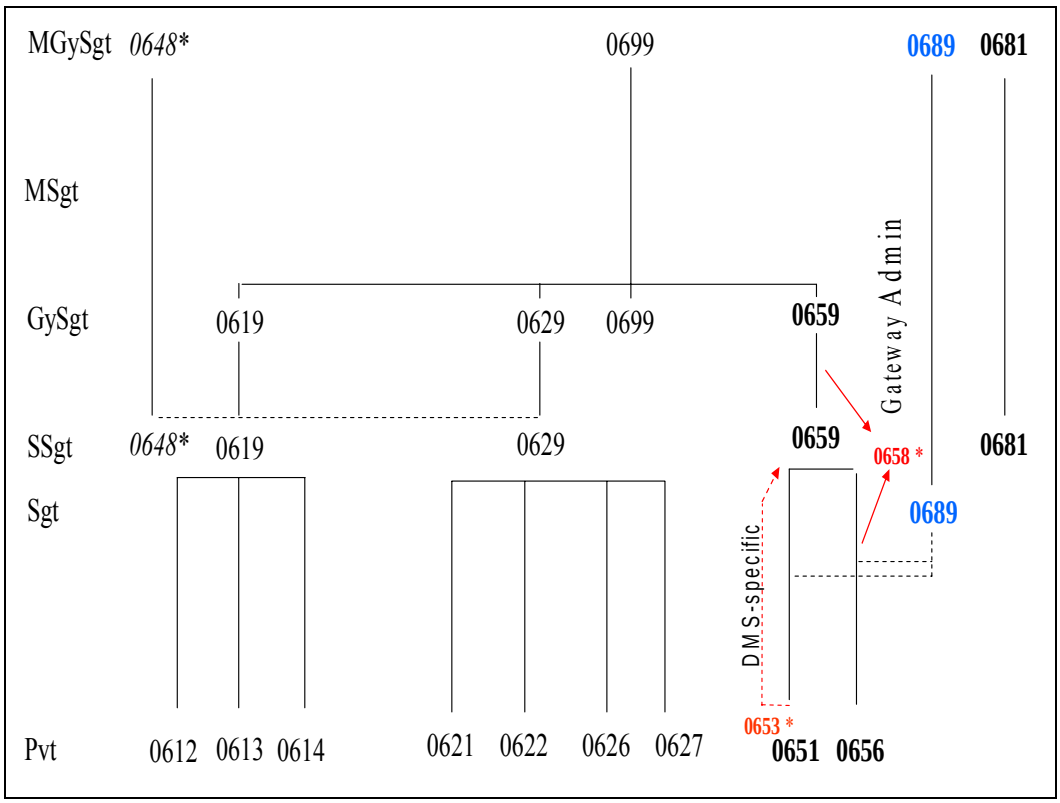
The computer field within the Corps has undergone a great upheaval in the last several years, with new Military Occupational Specialties (MOS's) being created and other MOS's being phased out. This business process re-engineering has effected all Marines within the computer MOS's. What used to be a steadfast MOS and a great stepping-stone to corporate America has vanished, to be replaced with an ambiguous MOS and less then desired training.

In 1995, Marine Corps Order 1510.37C was published, that detailed the Individual Training Standards (ITS's) for the Data Systems Occupational Field 4000. These ITS's provide a common base of training for all Marines who have the same MOS. ITS's are used to determine the proficiency of individual Marines and to establish training plans and courses of instruction. Marines are required to achieve proficiency as individuals in support of their unit combat missions.

The Marine Corps Combat Communications Electronics School (MCCES) in 29 Palms, California conducts the initial training of Marines assigned an MOS of computer specialist. The different MOS's awarded upon completion of training include:

0612, 0613, 0614, 0621, 0622, 0626, 0627, 0651 & 0656. The below diagram is an Enlisted progression chart for the MOS's.

**Table 1: MOS Progression Chart**




(Dulaney 2003)

0612: Field Wireman

0613: Construction Wireman

0614: ULCS System Specialist

0619: Wire Chief

0621: Field Radio Operator

0622: Multichannel Sys. Spec.

0626: Fleet SATCOM Sys. Spec.

0627: GMF/LMST/SMART-T

0629: Radio Chief

0651: Data Network Spec.

0653, DMS Sys. Spec

0656: Tactical Network Sys. Spec

0658: Gateway Tech

0659: Data Chief

0681: InfoSec Technician (EKMS)

0689: Information Assurance Technician

Within these MOS's are the corporate SAs of the Marine Corps. System administrators will usually have one of the following MOS's:

0651 – Data Network Technician

- Install, operate, and maintain network information systems in both a stand-alone and client-server environment.
- Plan, configure, and execute the integration of multiple information systems in a network environment; evaluate and resolve customer information systems problems; and effect required hardware/software upgrades and repairs to maintain mission capability, which includes MS Exchange, Defense Message System, and other authorized information systems.

0656 – Tactical Data Network Technician

- Install, operate, and maintain tactical data network systems. This will include installing and configuring hubs, routers, bridges, various transmission media; installing and configuring server hardware and software; and coordinating with the Data Network Technician to ensure proper installation and configuration of workstations.
- These Marines will also operate the Tactical Data Network (TDN) server.

0658 - Tactical Data Network Gateway Systems Technicians

- Install, operate, and maintain tactical networks to include in-depth support not limited to maintaining system software, hardware, and advanced LAN / WAN configuration concepts and implementing advanced communication concepts utilizing various tactical communication devices.

- They also execute network planning, network security, maintain patch panels, power entry panels, signal entry panels and the configuration of routers, switches, various encryption devices, and network monitoring software.
- This MOS is awarded only to Marines holding Primary MOS (PMOS) 0656 or PMOS 0659.

  0659 – Data Chief
- Data chiefs perform advanced systems installation, operation, integration, and troubleshooting in order to maintain optimum data communications systems operations.
- Data chiefs plan and supervise installation, configuration, and maintenance of all data communications systems and network services, including the Defense Message System (DMS), in both a garrison and deployed environment.
- They also plan and design Local Area and Wide Area Networks, link heterogeneous networks through the application of appropriate data and telecommunications hardware and software, develop and execute plans for tactical data communications systems and database integration and develop instruction for data network personnel in information technologies systems techniques and equipment employment.

  0689 – Information Assurance Technician
- Information Assurance Technicians are responsible for all aspects of ensuring Marine Corps information system's data availability, integrity, authentication, confidentiality, and non-repudiation.
- Single POC for all matters relating to data network security.

- Implement and monitor security measures for USMC communication information systems networks, and ensure that systems and personnel adhere to established security standards and governmental requirements for security on these systems.
- Duties include assisting in the development and execution of security policies, plans, and procedures; design and implementation of data network security measures; network intrusion detections and forensics; information system security incident handling; and certification of Marine Corps systems and networks.

Typically, Marine Corps System Administrators receive formal school training, and are tracked via MOS through the MOS progression. For this study, it is submitted that in accordance with the CJCSM 6510.01, the levels of System Administrators in conjunction with the Marine MOS's are as follows:

SA Level 1 – 0651/0656/0659 E1-E5

SA Level 2 – 0659/0689 E-5/E-6

SA Level 3 – 0689 E7-E9

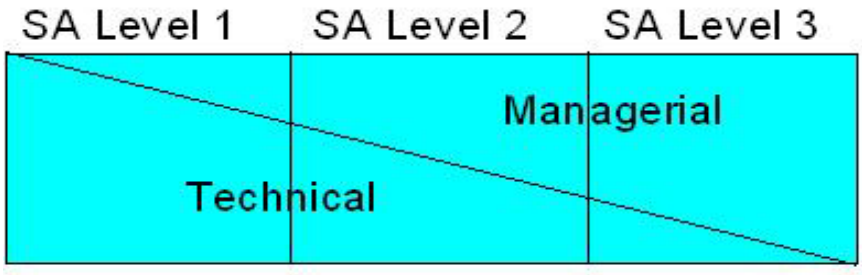



**Figure 6: System Administrator Levels**

## 2.11 Private Sector Certifications

Certification offers a benchmark for IT managers to assess their System Administrators knowledge, skills and abilities.

Certification requires intense preparation and study. In a Thompson Prometric Survey, (Thompson Prometric, 2002), respondent's attitudes agreed that there are certain benefits of certification:

- Certification is a great achievement-the result of hard work and personal sacrifice.
- Certification boosts self-confidence.
- Professional growth will increase if certified.

There is a significant perceived value in industry IT certifications. This perceived value requires a commitment for the potential student. Certification is not a task to be taken lightly. This type of training requires intense preparation and study. The failure rate for an initial test is almost 50%. (Ashe, 2004)

After a failure, there is a mandatory 6-month wait before being allowed to retest. In addition to the failure rate are the high costs of training. A+ exams cost $140 for individuals who are CompTIA members and $190 for non-members. These test costs are not included in the actual training costs to prepare for the tests. Typically, candidates who self-study, will spend $80 on books, which may include two study guides at $40 each or a $50 study guide and a $30 exam cram. Candidates also spend $70 on a practice exam, which usually includes enough questions for two or more distinct attempts at the exam. This permits the first take to be used for self-assessment to help guide study and

the second (and subsequent attempts) to provide a measure of readiness. This totals to be in the range of $300 to $500 per course.

**Table 2: Average Cost of Certification**

| # of Exams | Vendor | Direct Costs | # of Hours | Self-Study | CBT/Online | Classroom/ILT |
|---|---|---|---|---|---|---|
| | Microsoft | $100 | 60 | $250 | $480 | $1,750 |
| 5 | MCDBA | 500 | 300 | 1,250 | 2,400 | 8,800-13,800 |
| 4-7 | MCSE | 400-700 | 240-420 | 1,040-1,820 | 1,920-3,360 | 7,040-19,320 |
| 4 | MCSD | 400 | 240 | 1,040 | 1,920 | 7,040-11,040 |
| | Novell | 100 | 60 | 260 | 480 | 1,760-2,760 |
| 5-6 | CNE | 500-600 | 300-360 | 1,300-1,560 | 2,400-2,980 | 8,800-16,560 |
| 4-6 | MCNE | 400-600 | 240-360 | 1,040-1,560 | 1,920-2,980 | 7,040-16,560 |
| | Oracle | 125 | 80 | 285 | 505 | 1,785-2,785 |
| 4-5 | DBA | 500-625 | 320-400 | 1,140-1,425 | 2,020-2,525 | 7,140-13,800 |
| 5 | Developer | 650 | 400 | 1,450 | 2,550 | 8,800-13,800 |
| | Cisco | N/A | N/A | 250-460 | 560-660 | 1,750-2,960 |
| 1 | CCNA | 100 | 80 | 250 | 550 | 1,750-2,750 |
| 2/4 | CCNP | 300-400 | 320 | 900-1,000 | 1,500-1,600 | 6,900-11,000 |
| 2/4 | CCDP | 300-400 | 320 | 900-1,000 | 1,220-2,240 | 6,900-11,000 |
| 2 | CCIE | 1,550 | 400 | 2,190 | 2,790 | 4,690-6,690 |
| | Prosoft CIW | 125 | 50 | 285 | 585 | 1,785-1,785 |
| 7 | Developer | 875 | 350 | 1,925 | N/A | 12,425-19,425 |
| 4 | Administrator | 500 | 200 | 1,100 | 2,090 | 7,100-11,100 |
| 2 | A+ | 280-380 | 80 | 430-530 | 830-930 | 3,430-5,430 |
| 1 | SANS GSEC | 425 | 80 | 725 | 1,595 | 1,595 |
| 1 | SANS Level2 | 1,500-2,500 | 80 | N/A | 1,500-2,500 | 1,500-2,500 |
| 1 | SSCP | 295 | 60 | 595 | 895 | 2,095-3,095 |
| 1 | CISSP | 395 | 100 | 695 | 995 | 2,195- 3,195 |

CBT's cost on an average of $200. Actual price ranges may be as low as free or as high as $500 or more, depending on the vendor. $200 was used per exam topic as the metric to calculate costs for this approach.

Instructor Led courses run from $300 per classroom day to as high as $500 per classroom day. Most A+ topics are covered in five to 10 days of classroom training, so although individual experience will vary somewhat from topic to topic, an average of 80 hours of preparation and exam time is typical for each A+ exam. A+ requires two exams and usually takes 10 days of training. (Tittell, 2004)

Due to the increasing popularity of IT certifications in private industry, this research hopes to illuminate the perceived value of certification. Education or curriculum development is critical to establishing system administration as a full-fledged profession

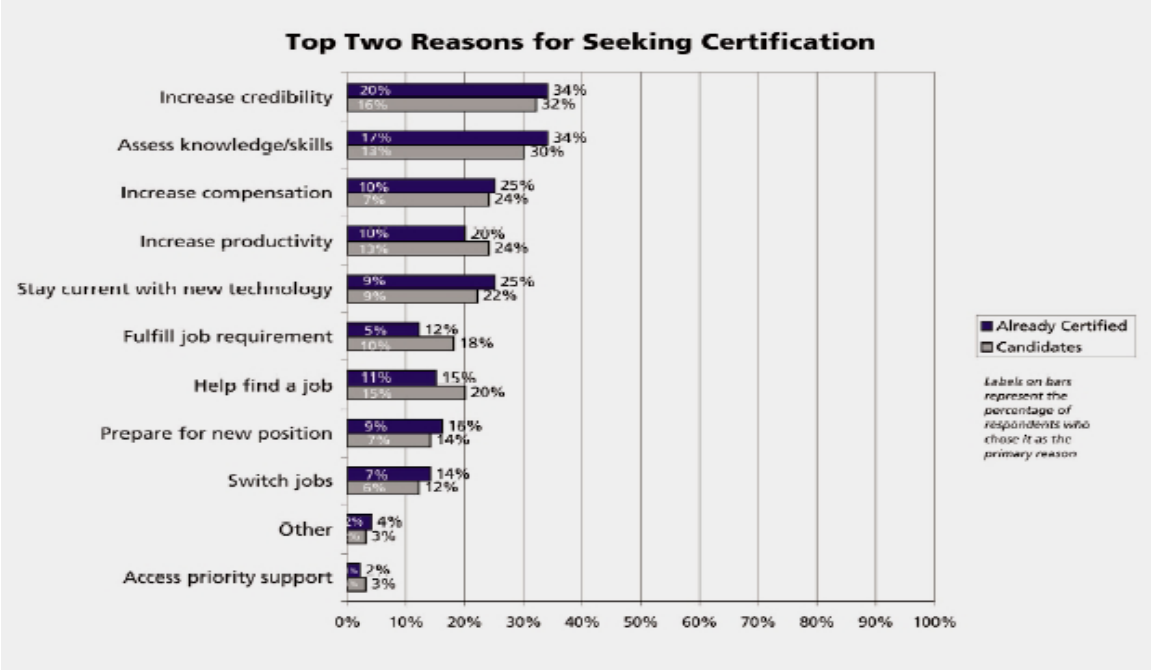



**Figure 7: Certification Seekers (Thompson Prometric, 2002),**

The quality of the training method, the existence of in-house training, and the availability of the training method are top factors that are used to select training for employees. (Thompson Prometric, 2002)

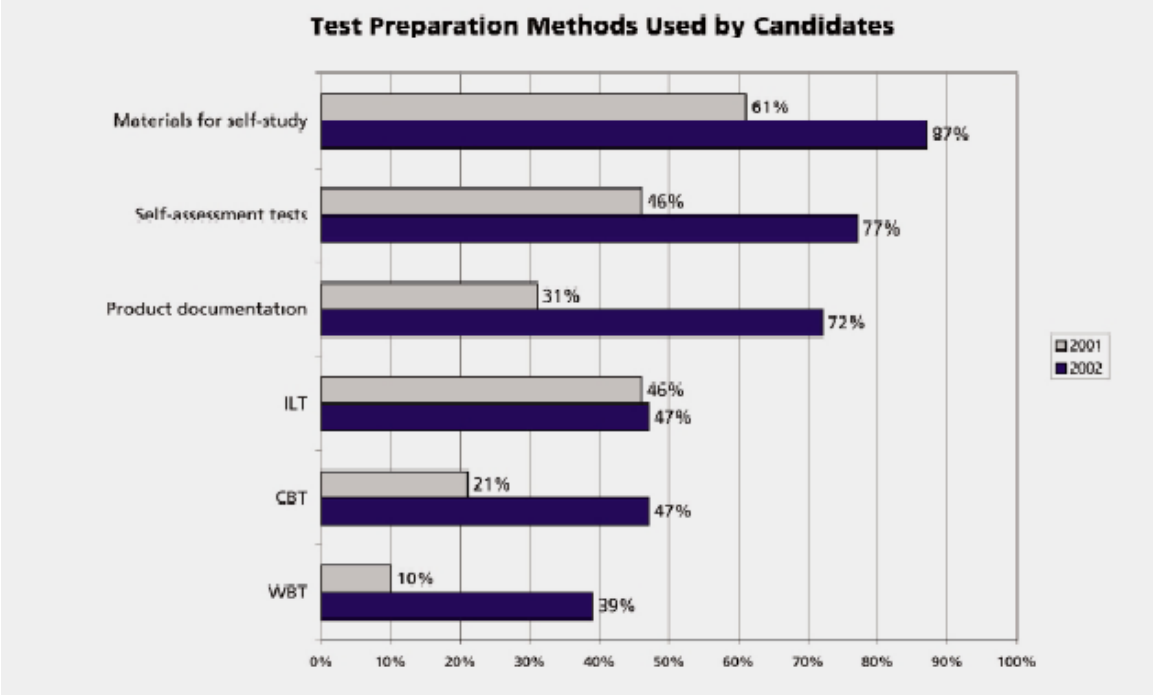



**Figure 8: Test Preparation Methods (Thompson Prometric, 2002)**

Figure 9 clearly indicates self-study is the main method for preparing for certification testing. Surveys have shown that Instructor Led Training (ILT) and self-study are the 2 most common delivery methods for IT training. This fact is apparent in the Marine Corps, as Marines are continuously deployed, they are able to take their self-study materials with them into the deployed environment.

Once certified, personal recognition is the most prevalent reward from employers. Up to 74 % of employers feel certification has a positive effect on employee credibility with customers and clients. (Johns 2003). Many certification experts agree that being certified is one of the best ways to enhance a career in the field of Information Technology. Increasingly employers are seeking certified professionals. Certifications

show that being updated in a career field is a high priority. Certification saves employer's time, training, money, and effort.

The certification business is a multi-million dollar venture for certification providers. TechSkills in Austin Texas offers IT certification, business skills training and administrative medical training. IT training for individual, corporate and government clients is the company's mainstay. The company's IT curriculum includes Cisco, Linux, Microsoft and Oracle certifications, as well as specialized training in security and Web design. Their company's revenues were $2 million in 1999 and grew to $33 million in 2003. TechSkills is aiming for $70M in 2006. (Lemen 2004)

Calif.-based New Horizons Computer Learning Centers Inc. is one of the biggest IT training companies with annual revenues over $200M. This company had a 48 % annual growth rate in earnings per share and a 40% revenue growth rate for the past three years.

These growth trends indicate that while the training is expensive, individuals and corporations are willing to certify their people.

### 2.12 Training versus Education

The phrase *training and education* are commonly used in the military. Both phrases describe a process of learning. A distinction exists between training and education. The DoD makes the distinction that training involves the use of Knowledge, Skills and Abilities whereas education is insight and understanding. (Zafra, 1991)

Training and education are two of the most commonly recognized undertakings to increase human capability. This research uses the Marine Corps' definitions of training and education, as defined below.

Training is the building in of information and procedures; using the progressive repetition of tasks, the product of training is skill development and proficiency. Training is performance based and is typically measured by objective standards. This type of training is ideal for SAs for their position is a practical one that faces redundant day-today challenges.

Education is the drawing out of students to initiate the learning process and bring their own interpretations and energies to bear—the product of which is a creative mind. Educational objectives may be measured directly, but are often inferred from subjective testing or a sampling of student behavior over a period of time.

The main difference in these definitions emerges from the type of knowledge they seek to develop. Military training is generally geared towards increasing explicit procedural knowledge and reinforcing reliable application of skills. The desired outcome of training is consistent performance measured against established standards. Conversely, education seeks to instill an increased ability to apply concepts and skills in unstructured and unfamiliar situations. The results of education tend to be more implicit and more difficult to define as compared to training objectives.

When training and education are forged with experience, the learning is more complete. The below model identifies the principle actions and outcomes of learning.

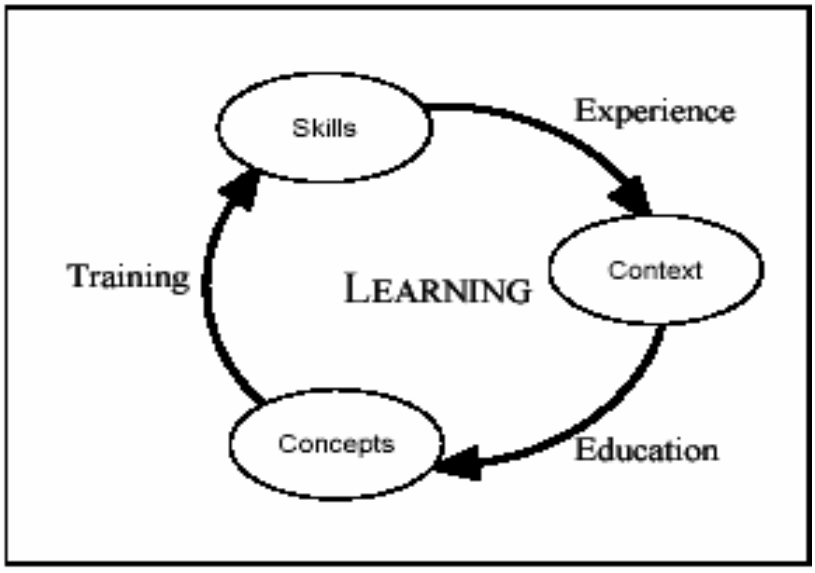



**Figure 9: Learning Model (Oser, 2002)**

Training tends to produce skills whereas education advances the learner's awareness of cognitive concepts. Each of these elements increase human capability and together, they provide a partnership to achieve greater intellect.

Within the realm of DoD, education is formal instruction at a college or university. If one receives classes or periods of instruction at a DoD school, this is deemed to be training. The SA, must understand all aspects of Systems Administration in order to be proficient in their roles, and regardless where they receive their training or education, all of this knowledge has to applicable to their role as a SA.

### 2.13 Mapping the Training Requirements

The objective to training and certification is to uphold and understand the principles and concepts of information and information systems protection. Another goal of training and certification is to subscribe to a standardized set of skills. This is the task

that has been mandated by the CJCSM 6510.01. Training alone is not considered sufficient criterion to optimize the security of information systems. The process begins with formal classroom training followed be on-the-job training and continues to being able to demonstrate competence in specific knowledge, skills and abilities.

To accomplish this task, the CJCSM 6510.01 has promulgated specific task sets that are required for System Administrators. These skill sets are based on the premise of Knowledge, Skills and Ability and fall within the construct of training in the below model.

Table 3: Human Factor in Training Strategies

| | AWARENESS | TRAINING | EDUCATION |
|---|---|---|---|
| **Attribute:** | "What" | "How" | "Why" |
| **Level:** | Information | Knowledge | Insight |
| **Learning Objective:** | Recognition and Retention | Skill | Understanding |
| **Example Teaching Method:** | Media<br>- Videos<br>- Newsletters<br>- Posters | Practical Instruction<br>- Lecture and/or demo<br>- Case study<br>- Hands-on practice | Theoretical Instruction<br>- Seminar and discussion<br>- Reading and study<br>- Research |
| **Test Measure:** | True/False<br>Multiple Choice<br><br>(identify learning) | Problem Solving, i.e., Recognition and Resolution<br><br>(apply learning) | Essay<br><br>(interpret learning) |
| **Impact Timeframe:** | Short-term | Intermediate | Long-term |

(Zafra, 1991)

These task/skill sets are broken down into three levels, Skill Levels 1, 2 & 3 SA. The subject areas include configuration control, operations and maintenance, incident response, operations monitoring and analysis; and countermeasures. The publications National Institute of Standards and Technology, (NIST) 800-16 and the National Security

Telecommunications and Information Systems Security Instruction, (NSTISSI), No 4013, provide the national training standards for system administrators. System Administrator certification is mandatory prior to issuing unsupervised root access.

Table 4: Skill Level 1 Requirements (CJCSM, 2003)

| **Knowledge** | **Skill** | **Ability** | **NIST Standard # 800-16** | **NSTISSI #4013** |
|---|---|---|---|---|
| Formal training on the OS and command language or network protocols/operating parameters (network administration). | | Understand computer operating system fundamentals. | | |
| | | | | |
| Know rudimentary system/network administrator tasks relevant to the OS or network device. | | Understand and perform basic OS tasks. | 2.2C | |
| | | | | |
| Know OS, command language, and/or network protocols. | Manage system hardware and software. | | 2.2C | 1 b<br>2 c |
| | Manage accounts. Maintain data store. | | | 2 d<br>5 c |
| | Provide communication connectivity and configure network protocols. | Install OSs, applications and peripherals; conduct testing and safeguards. | 3.3D<br>3.3E | 1 b<br>5 b |

Skill level 1 administrators usually have nominal experience (e.g., less than 3 years) in the job. Skill level 1 SAs are generally in the grades of E-3 to E-5 or civilian equivalent.

In the Appendix A, the CJCSM 6510.01 skill level requirements are presented. The first 3 knowledge requirements are shown in Table 3. The basis for training and certification is established by referencing the NIST 800-16 and the NSTISSI 4013.

Contained within these publications are specific skill sets that enumerate the skills that are required to be a System Administrator.

Table 4 illustrates how the NIST 800-16 has mapped the training requirements into a matrix. This System Administrator matrix is used in this research to identify specific training knowledge, skills and abilities. Table 4 shows in training area 1, Laws and Regulations, the functionality specialty a System Administrator is required to know is how to implement and operate within the prescribed laws and regulations. Cell 1D states, "— Individuals responsible for the technical implementation and daily operations of an automated information system are able to understand IT security laws and regulations in sufficient detail to ensure that appropriate safeguards are in place and enforced." (NIST 1998).

Individuals acquire different roles relative to the use of IT within an organization, or as they make a career move to a different organization. Sometimes they will be users of applications; in other instances they may be involved in developing a new system; and in some situations they may evaluate vendor proposals for IT systems. An individual's need for IT security training changes as their roles change. This is recognized within the learning continuum by segmenting the training level shown in Table 4 into six functional

specialties which represent categories of organizational roles: Manage, Acquire, Design and Develop, Implement and Operate, Review and Evaluate, and Use. A seventh category, "Other," is a place holder, to allow the matrix to be updated to accommodate any additional functional roles identified in the future. (NIST 800-16)

**Table 5: System Administrator Training Matrix**

| | | FUNCTIONAL SPECIALTIES | | | | | | |
|---|---|---|---|---|---|---|---|---|
| TRAINING AREAS | | A MANAGE | B ACQUIRE | C DESIGN & DEVELOP | D IMPLEMENT & OPERATE | E REVIEW & EVALUATE | F USE | G OTHER |
| 1 | LAWS & REGULATIONS | | | | 1D ✔ | | | |
| 2 | SECURITY PROGRAM | | | | | | | |
| 2.1 | PLANNING | | | | | | | |
| 2.2 | MANAGEMENT | | | | 2.2D ✔ | | | |
| 3 | SYSTEM LIFE CYCLE SECURITY | | | | | | | |
| 3.1 | INITIATION | | | | | | | |
| 3.2 | DEVELOPMENT | | | | 3.2D ✔ | | | |
| 3.3 | TEST & EVALUATION | | | | 3.3D ✔ | | | |
| 3.4 | IMPLEMENTATION | | | 3.4C ✔ | 3.4D ✔ | | | |
| 3.5 | OPERATIONS | 3.5A ✔ | | 3.5C ✔ | 3.5D ✔ | | | |
| 3.6 | TERMINATION | | | | 3.6D ✔ | | | |
| 4 | OTHER | | | | | | | |

(NIST 1998)

## 2.13 Summary

Information assurance (IA) practices across DOD are still in their infant years across DoD. Threats from inside and outside the perimeters are a constant reminder of the battle that SAs fight on a daily, weekly, monthly basis. The inherent MOS structure that the Marine Corps employ's acknowledges that continuous training must occur for System Administrators to stay abreast of the latest cyber threats. This continued training is cultivated by the DoD and the Federal Government by their establishment of a standardized set of Knowledge, Skills and Abilities that all SAs must possess before given access to the network. By exploring, defining and executing these benchmark skill sets, the Marine Corps can continue to meet the challenges of today's net-centric warfare environment.

The proposed research model for this study is presented in Chapter 3. The factors that impact the training of System Administrators may provide insight to designing potential solutions. Chapter 4 will detail the analysis of the data, and Chapter 5 will discuss the research findings, any limitations, as well as recommendations for further research in to this area.

# III. Methodology

## 3.1 Introduction

The previous chapters discussed the lack of benchmark training for System Administrators across the Marine Corps. Additionally examined was the increasing need for Information Assurance across the DoD enterprise along with a continuous need for training. Background information on the concepts of Information Assurance, IT training and Education were also examined. The proposed theory is that the System Administrators are receiving different training from different sources with no benchmark training being conducted that meets the requirements set forth by the CJCSM 6510.01.

This chapter will outline the methodology to investigate the training methods used and the relationship between the quality of the training, the percentage of training received in specific areas and where the training was received. It includes a description of the population under study, survey instrument development, data collection methods, and the statistical techniques that will be used to analyze the data.

## 3.2 Research Approval

Permission to conduct this research was granted by the Air Force Personnel Center's Survey Branch (AFSB) in accordance with Air Force Instruction (AFI) 36-2601, which requires all Air Force surveys be approved and assigned an Air Force survey control number. The survey was also reviewed by the Human Subjects Review board. An exemption to AFI 40-402 was requested and granted by the Air Force Research Laboratory Human Effectiveness Directorate 17 December 2002. The survey was assigned F-WR-2004-0021-E as the Case Log Approval number.

### 3.3 Population

The population for the study consists of Active Duty System Administrators throughout the Marine Corps. This includes all ranks, and is not limited to specific career fields, as long as respondents have been System Administrators. Participation in the experiment was strictly voluntary. All the participants had at least a high school degree, and some had obtained higher levels of education. The sampling strategy used for this research was cluster sampling. The population of interest is typically spread out over a large area, (e.g., worldwide military assignments). It is not feasible to use other sampling strategies through normal randomization procedures. The Marine Corps has identical billet assignments by major command Table of Organization. This made cluster sampling a reasonable strategy..

#### 3.3.1 Sample Size

The expected sample size is 370 derived from the calculations provided in Table 4. Gay (1989) has suggested the following guidelines for selecting a sample size:

- For populations (N<100), survey the entire population.
- For populations (N= 500), 50% of population should be sampled.
- For populations (N= 1500), 20% of population should be sampled.
- For populations (N>5000), sample size should = 400.

The sample size for this research is derived from the following figures:

**Table 6: Expected Sample Size**

| | |
|---|---|
| 2759 | Total Table of Organization (T/O) Active Duty 0651 & 0656 MOS |
| - 551 | 20% below actual T/O Level. (80% staffing goal.) |
| 2208 | Actual # of 0651 & 0656 personnel on hand (HQMC 2003) |
| -662 | 30% of Population in deployed status. (HQMC 2003) |
| 1546 | Total available for System Administrator duties. |
| -309 | Only 20% of available SAs are full time administrators.<br>(Limited # of SAs that have root level access) |
| 1236 | Total available for survey |

Since no data is readily available on current e-mail addresses of this entire population, the survey was sent out to Supervisors and Department heads with directions to disseminate the survey down to the lowest levels.

### 3.4 Survey Instrument Development.

The following sections describe the process that was undertaken during the Pilot Study. The demographics and career filed descriptions are explained along with the resulting modifications to the survey.

#### 3.4.1 Pilot Study

Students in a graduate program in information resource management were invited to test the instrument prior to the pilot study. This group was asked to complete

the survey and to report any concerns or problems they experienced. 15 students completed the questionnaire and provided constructive feedback regarding the nature of the questions and the format of the survey. Some content of the survey was modified after the student test. The feedback also addressed minor technical problems and the survey format, such as respondents being able to select two answers for one question.

After the changes recommended from the student test were implemented, a sample of System Administrators assigned to Camp Lejeune, North Carolina, pilot tested the instrument. The pilot study replicated the administration of the survey to the greatest extent possible. Specifically, an e-mail message was sent to 25 System Administrators inviting them to participate in the study. A follow-up message included an Internet link to the survey. The pilot test was conducted for an 10-day period beginning 15 November 2003.

At the conclusion of the pilot study, 16 System Administrators had completed the survey. When the original invitation was e-mailed to participants, five messages were returned as undeliverable and four participants did not respond. Therefore, the overall response rate for the pilot test was 64%. Pilot study participants were enlisted Marines ranging in rank from Lance Corporal, to Master Sergeant, E-3 to E-8. All participants were from the 06 Computer career field. They were assigned to 12 different units ranging across 3 organizational levels, and included Marine Corps Base, 2d Marine Division and 2d Marine Expeditionary Force. 12 of the participants were assigned to System Administrator positions at the time they completed the survey, or had been assigned to similar positions in the past.

### 3.4.2 Survey Modifications

The feedback received from the student and pilot tests was beneficial. After the student test, minor technical glitches were remedied. After the pilot test, changes were made to the specific wording on two questions. First, additional guidance was added to the "What unit are you presently attached to?" question. In the pilot study responses, some participants included their full office symbol (2MEF, G6, Security Branch, and MCB, G6, IA Section), while others only listed their parent unit (2MEF, MCB, 2MARDIV). Hence, the question was changed to read as follows: "What unit are you presently attached to?" with the only options in the drop down menu being Major Commands.

Second, realizing that the System Administrator population contains Active Duty military both enlisted and officer, an additional block of "other" was added for the Rank/Pay Grade input.

### 3.4.3 Survey Construct

Based from the training requirements presented in the CJCSM 6510.01 and NIST 800-16, there were 25 questions posed on the survey. Survey questions are presented in Appendix A. These questions are designed to evaluate the level of knowledge that current Marine SAs have.

The emphasis of the Training Requirements within the System Administrator training matrix is on training criteria or standards. The Learning Continuum presented in NIST 800-16 and in Chapter 2 of this study, shows the relationship among Awareness, Security Basics and Literacy, Training, and Education. This Continuum demonstrates that

Awareness and Security Basics and Literacy form the baseline which is required for all individuals involved with the management, development, maintenance, and/or use of IT systems.

CJCSM 6510.01 lists the following training requirements for Skill 1 SA. These training requirements are mapped to the NIST 800-16. The NIST 800-16 breaks these requirements down into a matrix with the specific cells as follows:

1D, 1E, 2.1B, 2.1C, 2.2C, 2.2D, 3.1C, 3.2B, 3.3C, 3.3D, 3.3E, 3.4D, 3.5D.

3.2D, 3.4C, 3.5A, 3.5C & 3.6D

### 3.5 Survey Instrument

The final survey was disseminated by e-mail to a variety of MOS's within the 06 Computer Field. These occupational fields contain a large majority of the System Administrators throughout the Marine Corps. The survey consists of a series of five web pages that are made up of checkboxes, rating buttons, and short answer fields that populate a database. The survey response period was 26 (6 January 2004 through 31 January 2004). There were 25 total questions.

#### 3.5.1 Demographic Information (Survey questions 1-6)

The remainder of this section describes the format and objective of the demographic survey pages. The first 2 pages of the survey collects demographic information about the respondent.

**Table 7: Survey respondent information**

| Section | Rationale |
|---|---|
| Respondent background information:<br>MOS<br>Unit attached to<br>Rank | Record respondent information for further data collection. Demographic data used to provide an option to divide population by MOS & Rank. |
| Job information, Certification information & Education level:<br>Primary Job<br>Yrs of Experience<br>System Environment (e.g. how many users, etc.)<br>Certifications<br>Education level | Data used to sub-divide subject population. |

The survey poses specific questions that were derived from NIST Security Standards. The responses to these questions are designed to measure three areas; how the training was delivered, (e.g. formal school or On-the-Job training), what percent of the training was received for each delivery method and the quality of training. A NIST security question is presented and the responder has to fill in three areas about the specific question. For example, question 2 states - "Understand physical security principles". The responder is then given seven different choices of where they received their training in this specific area: Military Occupational School (Formal school), On-the-Job training, College, Certification training, Self-taught, Web-Based Correspondence training or local command training. The responder is only allowed to choose the two choices that had the greatest percentage of how they received their training for that specific area. The percentages should add up to 100%.

Although it is recognized that a majority of training is a combination of the categories, responses are required for only 2 categories for each question; whichever 2 categories had the greatest percentage of learning the area in question.

The key to addressing people factors or competencies is awareness, training, and education. The questions contained in the survey examine training criteria and were established according to System Administrators roles within their organizations. (NIST 800-16).

### 3.5.2 Certification Information (Survey Questions 7-10)

Survey questions 7-10 are specifically related to the most common IT certifications the respondent might typically possess. Traditionally Marine Corps IT professionals seek private sector certification as a means to enhance their skills and to attain a coveted certification.

The driving factor behind certification is continued training. 22% of IT managers indicate they will purchase more training materials then in previous years while 37% state they will spend the same amount as in previous years. (Ashe, 2000)

## 3.6 Data Collection Method

Survey information was recorded via web-based questionnaires. Using an Internet web-site (http://en.afit.edu/HamiltonSurvey.xls) to collect the research data provided advantages. This method not only allowed for an organized presentation of the instruments and minimal paper use, but it also allowed the responses to be directly transferred to a database for analysis.

### 3.7 Hypothesis Development

CJCSM mandates that System Administrator training must be conducted. However, it is left up to the military departments on how to conduct the required training. Currently within the Marine Corps, the System Administrator population continues to grow. Information systems continue to become heavily dependent on the skill sets of System Administrators. The risks to the DoD's information resources are well known and the strengths of the information infrastructure defenses are being tested daily. *The weakest link in those defenses is not the technology but the people who use, administer, and manage it.* (de Zafra 1991).

#### 3.7.1 Hypothesis 1

Preliminary investigative research indicates that the training delivery mechanism is not consistent throughout the enterprise. The asymmetric nature of the training is disparate across geography, organization structure, and rank. Hypothesis one will attempt to ascertain how much of the required skill sets is attained through formal schooling. Since no prior documentation exists to identify the portion of required training that is received through formal schooling, a 50 percent level will be assumed.

**$H_1$**: 50 % or more of System Administrator training is provided through formal military schooling.

**$H_{1a}$**: Less than 50 Percent of System Administrator training is provided through formal military schooling.

### 3.7.2 Hypothesis 2

Preliminary investigative research has also identified a variety of training delivery methods for System Administrators. Since the variety is great, this research only seeks to identify those that are being utilized by more than 10 % of the population. A 10 % threshold was selected due to the traditionally low response rate of web-based surveys. The final training delivery methods selected are classified for this study as indicated in Table 7.

**Table 8 Training Delivery Methods**

| Formal School | Other Training Method |
|---|---|
| MCCES | On-the-Job Training |
| CCSS | College |
| FSA | Certification |
| PAS | Distance Learning |
| | Marine Corps Institute |
| | Local Command |
| | Self Taught |

In order to ascertain the usefulness of the training in regards to the functional duties of System Administrators, a quality component was included in the survey instrument. Data regarding quality of training are largely opinions or estimates by respondents; these are subject to inaccuracy and bias. (Neacy 2000) The most precise way to measure and improve the quality and effectiveness of training is through a return on investment (ROI) analysis of training programs. Without an ROI analysis being conducted, the perception of the quality of training may be examined instead. (Worthen, 2001), An individuals' perception of the quality of training is a metric that can be used for gauging the appropriateness of the training received.

Regardless of the distribution of the training methods, the quality perspective provides an informative measure of which training method is meeting the actual demands of System Administrator duties. For these reasons, the quality of training factor has been included in the survey instrument in the form of a 5-point Likert scale.

**$H_2$**: There is no difference in the quality of training methods between formal schools and other training.

**$H_{2a}$**: There is a difference in the quality of training methods between formal schools and other training.

### 3.8 Contingency Table Analysis

The data of this study consists of different categorical variables such as the different delivery methods used, e.g., MOS, OJT. This data is categorical data. The variables can take one of two or more values or levels, but the values are not considered to have any ordering.

In order to analyze associations between categorical data, a contingency table analysis can be used. Contingency table analysis provides an instrument for analyzing possible relationships between nominal data with more than two outcomes.

Contingency tables are a two-way table that is formed when considering two discrete variables. For a data set of *n* observations classified by the two variables with rows and columns, *r* and *c* respectively, a two-way table of frequencies or counts with *r* rows and *c* columns can be computed. A graphical representation if provided in Table 8.

**Table 9: Contingency Table Analysis**

| | | | |
|---|---|---|---|
| $n_1$ | $n_2$ | $n_3$ | $n_1$ |
| $n_{21}$ | $n_{22}$ | $n_{23}$ | $n_2$ |
| $n_{31}$ | $n_{32}$ | $n_{33}$ | $n_3$ |
| $n_1$ | $n_2$ | $n_3$ | $n$ |

If individual values are cross-classified by levels in two different attributes such as delivery method and quality , then a contingency table is the tabulated counts for each combination of levels of the two factors, with the levels of one factor labeling the rows of the table, and the levels of the other factor labeling the columns of the table. The counts for each cell in the table would be the number of subjects with the corresponding row level of delivery method and column level of quality. (Agresti 1996)

Using contingency table analysis, the null hypothesis assumes that the two classifications are independent. The test for independence is conducted by comparing the actual cell count to the expected cell count. This method is the chi-squared ($\chi^2$) test statistic, $\chi^2 = \sum_{i=1}^{i} \frac{(O_i - E_i)^2}{E_i}$, where $O$ is the number of observed counts and $E$ is the number of expected counts and $i$ is the number of rows and $j$ is the number of columns. Large values of $\chi^2$ indicate that the actual counts do not match the expected counts and the assumption of independence is likely false.

Pearson's chi-square test for independence for a contingency table tests the null hypothesis that the row classification factor and the column classification factor are independent, (Connor 2003). The chi-square test for independence compares observed and expected frequencies (counts). The expected frequencies are calculated by assuming

the null hypothesis is true. The chi-square test statistic is basically the sum of the squares of the differences between the observed and expected frequencies, with each squared difference divided by the corresponding expected frequency. Note that the chi-square statistic is always calculated using the counted frequencies.

The distribution is arrived at under the assumption that the expected cell frequencies, are not too small, thus the degrees of freedom are approximately, a $\chi$2-distribution with $(c - 1)(r - 1)$.

In order for contingency table analysis to be valid, there are assumptions made. First is that the n observed counts are a random sample from the population of interest. Secondly, the sample size, n, will be large enough so that the expected cell count will equal 5 or more. An expected cell count of less than 1.0 for any cell is unacceptable.

Other assumptions with chi square tests:

- Adequate cell sizes are assumed. A common rule is 5 or more in all cells of a 2-by-2 table, and 5 or more in 80% of cells in larger tables, but no cells with zero count.
- Independence. Observations must be independent.
- Similar distribution. Observations must have the same underlying distribution.
- Known distribution. The hypothesized distribution is specified in advance, so that the number of observations that are expected to appear each cell in the table can be calculated without reference to the observed values.
- Non-directional hypotheses are assumed. Chi-square tests the hypothesis that two variables are related only by chance.
- Finite values. Observations must be grouped in categories.

- Normal distribution of deviations (observed minus expected values) is assumed. Chi-square is a *nonparametric test* in the sense that is does not assume the parameter of normal distribution for the data -- only for the deviations.
- Data level. No assumption is made about level of data. Nominal, ordinal, or interval data may be used with chi-square tests.

### 3.9 Summary

This chapter described the research design and methodology used to investigate the training methods used and the relationship between the quality of the training, the percentage of training received in specific areas and where the training was received. It included a description of the population under study, survey instrument development, data collection methods, hypothesis questions and the statistical techniques that will be used to analyze the data.

The following chapter provides the analysis of the data collected by the Study of Training Methods Survey conducted in January 04. Chapter 5 will discuss the results of the analysis, limitations of the study, implications for the Marine Corps, and suggestions for further research.

# IV. Data Analysis

## 4.1 Overview

The previous chapters outlined the problem statement, reviewed literature pertaining to Information Assurance, System Administrators roles and responsibilities and training versus education. Previous chapters also presented the research questions and hypotheses tested in this study. In addition, chapter three outlined the methodology for collecting the data and the statistical methods to be used to analyze the data.

This chapter examines the results of the survey and describes the statistical process used to evaluate the data. Both hypothesis posited in Chapter 3 are analyzed using results of the statistical analyses.

To review, hypothesis 1 posited that System Administrators are receiving more then 50% of their training through military formal school. Hypothesis 2 posited that there is no difference in the quality in the delivery methods. These hypotheses are summarized again in Table 8.

**Table 10: Hypotheses Summary**

| *Hypothesis* | *Description* |
|---|---|
| Hypothesis 1 | 50 % or more of System Administrator training is provided through military formal schooling. |
| Hypothesis 2 | There is no difference in the quality of training methods between military formal schools and other training. |

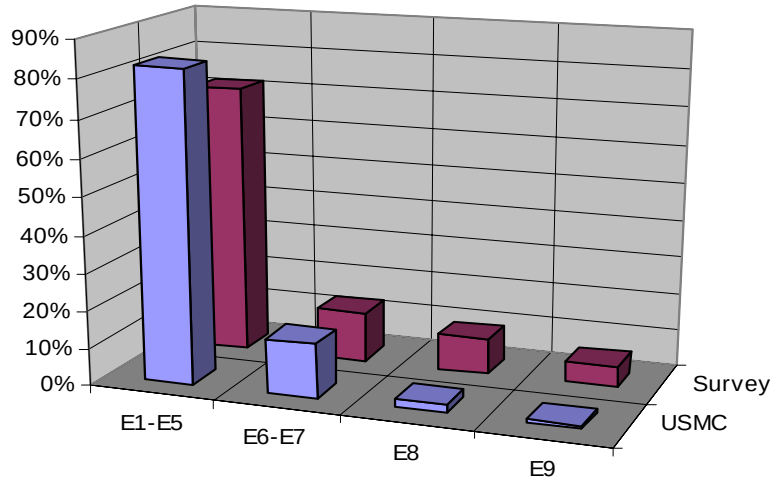
## 4.2 Survey Data Analysis

There are some inherent limitations to the analysis based on the available data. Only limited inferences can be made based on the low response rate of this research. Most of the limitations can be attributed to the small sample size (n=53). This is due to several factors; Operational tempo, e-mail failures, and the general lack of interest from the population. Previous surveys conducted by HQMC and DoD have met with similar results. (HQMC 2002)

As noted previously, the survey was intended for System Administrators from throughout the Marine Corps regardless of their geographic location. The overall response rate was only 4 % which limits the amount of inferences that can be made about the population.

## 4.3 Respondent Characteristics

Respondent demographic information is presented in Figure 10 and Table 11. Figure 10 illustrates the survey rank distribution compared to the Marine Corps' overall enlisted rank distribution. As shown below, the survey data closely matches the rank distribution of the Marine Corps. E1-E-5's typically make up 83% of the Marine Corps and in the sample these ranks were a relatively comparative 72%. (HQMC 2004)




| | E1-E5 | E6-E7 | E8 | E9 |
|---|---|---|---|---|
| USMC | 82.56% | 14.47% | 2.10% | 0.87% |
| Survey | 71.70% | 13.21% | 9.43% | 5.66% |

**Figure 10: USMC Demographics vs Survey Demographics**

Table 11 outlines the demographics of the survey respondents. Demographic information collected from respondents included unit assigned to, MOS, rank, job responsibilities, number of years working with computers, education, and age. A majority of the sample was from the 0651 MOS, with 71% of the sample being E1-E5's. The average age of the sample was 27 and the majority of the samples were assigned to Marine Corps Base.

**Table 11: Respondent Demographics**

| *Characteristic* | *n* | *%* | | *Characteristic* | *n* | *%* |
|---|---|---|---|---|---|---|
| **Age** (in years) | | | | **MOS** | | |
| < = 25 | 33 | 62.2 | | 0600 | 1.00 | 1.8 |
| >26 <= 35 | 8 | 1.8 | | 0681 | 1.00 | 1.8 |
| >= 36 | 12 | 22.6 | | 0651 | 22.00 | 41.5 |
| | | | | 0653 | 1.00 | 1.8 |
| **Rank** | | | | 0656 | 9.00 | 16.9 |
| E1-E5 | 38 | 71.7 | | 0659 | 2.00 | 3.7 |
| E6-E7 | 7 | 13.2 | | 3000 | 9.00 | 16.9 |
| E8 | 5 | 9.4 | | 0100 | 1.00 | 1.8 |
| E9 | 3 | 5.6 | | **Yrs of Experience** | | |
| **Unit Assignment** | | | | 1-3 Years | | |
| 1st MAW | 1 | 1.8 | | 4-6 Years | 28 | 52.8 |
| 2D FSSG | 4 | 7.5 | | 7-9 Years | 10 | 18.8 |
| 2d MARDIV | 9 | 16.9 | | 10+ years | 6 | 11.3 |
| 2d MAW | 1 | 1.8 | | **Education** | 9 | 16.9 |
| 3d FSSG | 3 | 5.6 | | AS | 7 | 13.2 |
| MCB | 32 | 60.3 | | HS | 37 | 69.8 |
| MEU/MEB | 3 | 5.6 | | BS | 1 | 1.8 |
| | | | | MS | 2 | 3.7 |

## 4.4 Hypothesis 1 Analysis

Hypothesis 1 stated that 50 % or more of System Administrator training is provided through formal schooling with the alternate hypothesis stating that less than 50 % of System Administrator training is provided through formal schooling.

Because the training delivery mechanism for System Administrator training is not consistent throughout the enterprise, Hypothesis 1 attempts to ascertain how much of the required skill sets is attained through formal schooling. A 50 percent level was assumed, indicating that at least 50% of System Administrators training is provided at their formal school.

To analyze the data, binomial statistics were used. The survey returned data from fifty - five subjects, with 2 responses being invalid, consequently, the number of valid responses is 106 as each respondent was allowed to pick 2 categories, whichever 2 categories attributed most to learning the area in question.

**Table 12: Cumulative Counts of Where 50% or more of training is being received.**

| QUESTION | Responses | MOS | OJT | Other |
|---|---|---|---|---|
| 1 | 104 | 11 | 27 | 66 |
| 2 | 106 | 15 | 29 | 62 |
| 3 | 106 | 11 | 27 | 68 |
| 4 | 98 | 7 | 27 | 64 |
| 5 | 98 | 7 | 19 | 72 |
| 6 | 100 | 11 | 20 | 69 |
| 7 | 102 | 12 | 28 | 62 |
| 8 | 96 | 6 | 21 | 69 |
| 9 | 94 | 9 | 20 | 65 |
| 10 | 98 | 5 | 17 | 76 |
| 11 | 94 | 6 | 22 | 66 |
| 12 | 100 | 6 | 17 | 77 |
| 13 | 102 | 14 | 16 | 72 |
| 14 | 92 | 9 | 21 | 62 |
| 15 | 100 | 10 | 20 | 70 |
| 16 | 92 | 4 | 16 | 72 |
| 17 | 102 | 12 | 23 | 67 |
| 18 | 98 | 9 | 20 | 69 |
| 19 | 104 | 13 | 21 | 70 |
| 20 | 98 | 8 | 28 | 62 |
| 21 | 96 | 17 | 21 | 58 |
| 22 | 98 | 11 | 20 | 67 |
| 23 | 96 | 7 | 30 | 59 |
| 24 | 96 | 7 | 22 | 67 |
| 25 | 100 | 4 | 21 | 75 |
| Total | 2470 | 231 | 553 | 1686 |

The data does not support the null hypothesis. Results clearly show that the alternate hypothesis is supported. The alternate hypothesis states that 50% or less of the System Administrator training received is at MOS school. The three highest responses for

MOS training were question # 2, 13, and 21. Their respective values were, 15, 14, and 17. Thus 15 respondents replied that they had received 50% or more of their training for question number 2 at MOS school. The alternate hypothesis is supported from the data shown in Figure 11. The data shown in Figure 11 are cumulative counts of the number of times respondents answered that they had received 50% or more of their training for the specific question.

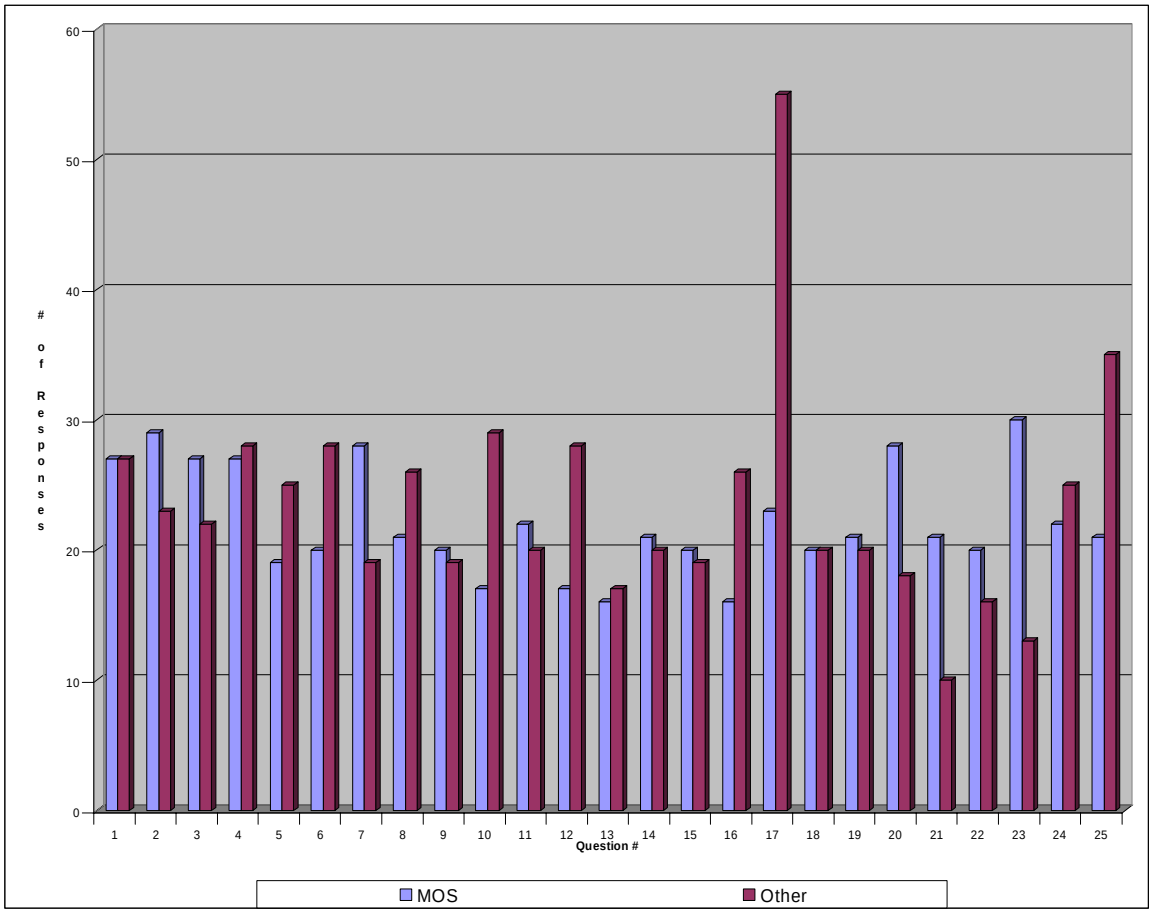



**Figure 11: Distribution of SA Training Delivery Method (Above 50%)**

Examining the distribution, anomalies exist in the data points that need to be explained. Survey Question # 6 states "Assist in access control security". This type of operation is locality dependent and while the topic may be covered briefly in MOS

school, the training for this process is more applicable to OJT, where specific local constraints are relevant. Question # 7 is "Know basic differences between deployed and garrison operating environments." This question is a procedural question that deals with the architecture of the network. While the architecture may vary to some extent from location to location, this topic is focused enough to be taught in MOS school. Questions # 10, 12, and 16 are also locality dependent and will have specific constraints applied based on location. These questions all received a high OJT response rate.

Question # 17 states, "Install OS's, applications and peripherals". With the ubiquity of computers in today's society, this task has become a mundane operation to most high school graduates. Table 13 illustrates that the majority of responses for this question fell in the Self-taught category. With such a high response rate, this indicates that this task is a relatively easy task to learn and execute.

**Table 13 : Question # 17 (Install OS's, applications and peripherals) Data**

| QUESTION | # of Responses | MOS | OJT | College | Cert | Self | Web | Cmd |
|---|---|---|---|---|---|---|---|---|
| 17 | 102 | 12 | 23 | 1 | 8 | 39 | 0 | 7 |

Questions 20, 21, and 23 are procedural questions that ask about security policies and procedures. This type of training is conducted at MOS school where Marine Corps IT policy and procedure is the foundation of the curriculum.

Table 14 demonstrates the distribution of the responses. Because a binomial distribution is used, only the successes or the responses 50% or greater are analyzed.

There were a total of 2470 responses but only 1372 responses were considered successes, or met the success threshold of 50% or more. Out of these 1372 responses, only 231 responses were received for MOS training. This shows that only 17% of the training was received at formal military MOS school. This data does not support the null hypothesis.

**Table 14: Distribution of Counts Equal to and Above 50% & Below 50%**

| MOS | OJT | COL | CERT | SELF | WEB | CMD |
|---|---|---|---|---|---|---|
| 231 | 553 | 23 | 155 | 264 | 14 | 132 |
| 17% | 40% | 2% | 11% | 19% | 1% | 10% |

Figure 12 is a graphical representation of the distribution of the responses. All responses represented in Figure 12 were responses for 50% or more. For ease of data translation, the data is shown by the actual category, MOS, OJT, Self-Taught, etc. All categories for Hypothesis 1 were coded into two categories for Hypothesis testing, MOS and Other. Responses that fell below 50% were not included in this graphic. As graphically represented, OJT training was the biggest contributor to training that System Administrators receive. The second highest rated category where training was received is the self-taught category. MOS training finished 3rd with only 17%. These percentages address investigative question 1.

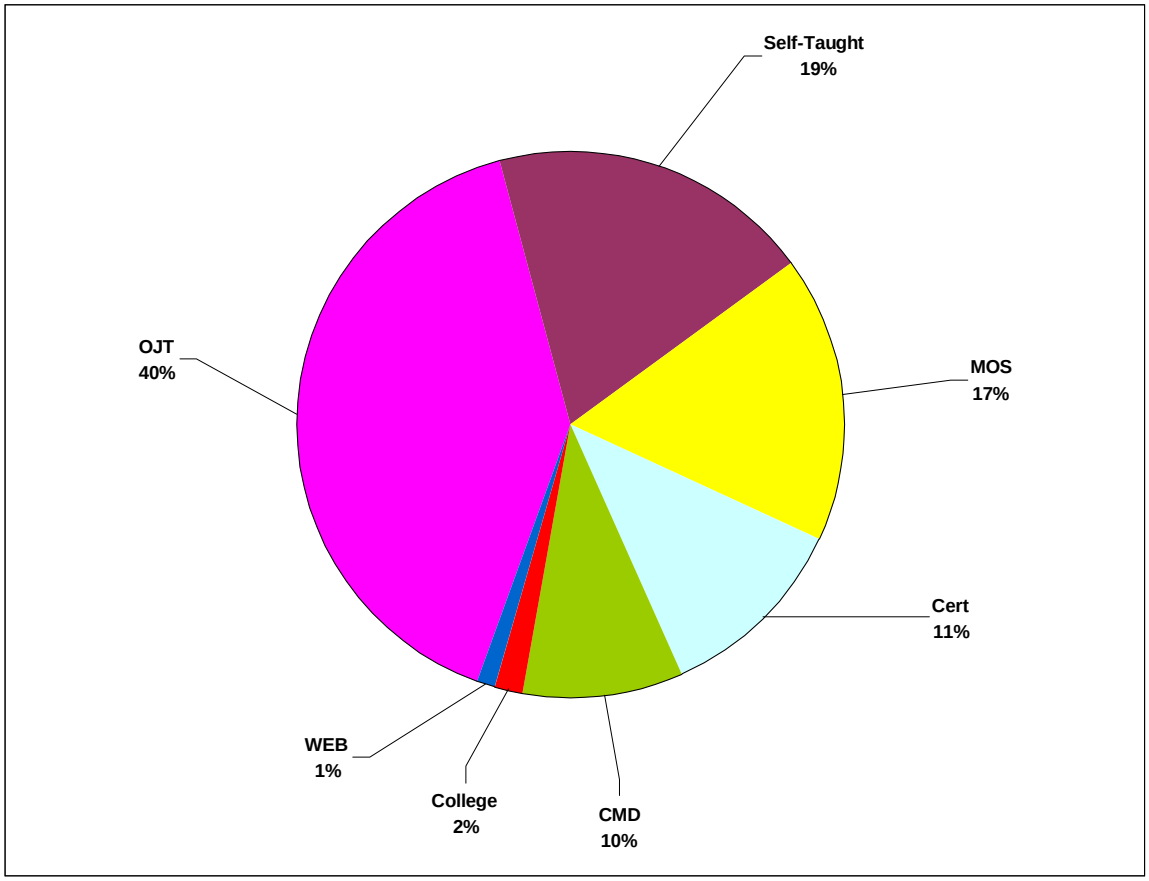



**Figure 12: Distribution of Training Delivery Methods**

### 4.4.1 Investigative Question 1

Investigative question 1 is a follow-on question to Hypothesis 1. Investigative question 1 posits the question "Where is the training for System Administrators being conducted". Figure 12 clearly shows that the majority of training is being received via OJT.

There are several problems with OJT. The principal difficulty is the lack of consistency across the Marine Corps Enterprise in OJT. This lack of consistent skill set is also the driving problem behind the local command (CMD) training. The other problem is the lack of commitment of the trainer to conduct OJT. (Wagner 1998)

Although OJT is inconsistent across the Marine Corps, this training method is still a practical method because it is planned, organized, and conducted at the System Administrator's worksite. OJT is generally the primary method used for broadening skills and increasing productivity. It is particularly appropriate for developing proficiency skills unique to a System Administrators job - especially jobs that are relatively easy to learn and require locally-owned equipment and facilities. (DOI, 1998). Many OJT programs are developed as an integral component of the overall technical and skills training program throughout the unit.

The second highest rated training delivery method was Self-Taught Training at 19%. Once again, the principal difficulty is the lack of consistency across the Marine Corps Enterprise. The lack of consistent skill set is a problem that has been defined throughout DoD for decades.

### 4.4.2 Investigative Question 2

Investigative question 2 asks are private industry certifications an alternative method that can be used for DoD System Administrator certification?

As previously discussed in Chapter 2, certifications are a common goal among IT professionals. Figure 13 illustrates the currently held certifications by the survey respondents.

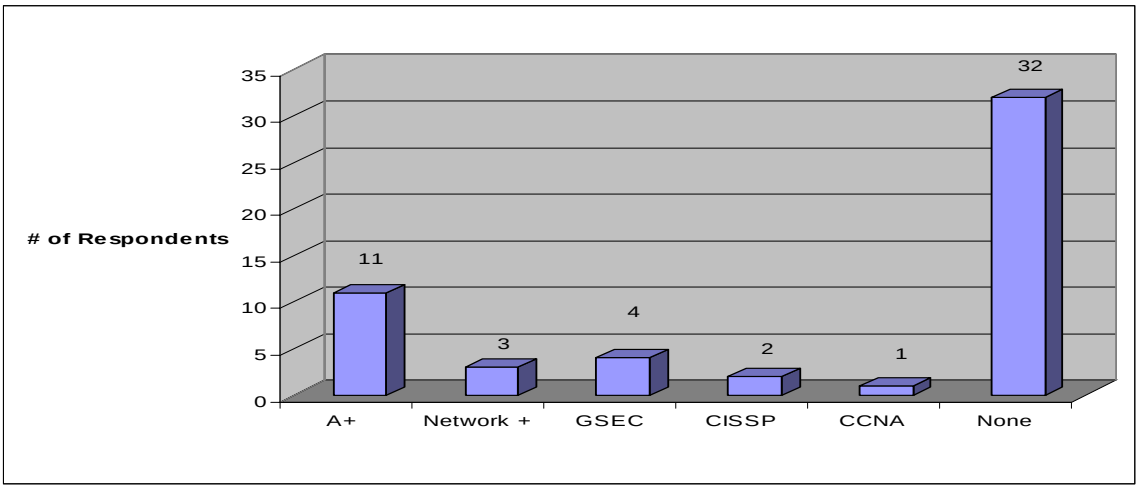



**Figure 13: Currently Held Certifications**

Figure 14 depicts that 77% of Marine Corps System Administrators are willing to re-enlist or extend their service obligation in return for certification training and examinations. This graphic echoes what private sector IT professionals are also vying for, a chance to become certified.

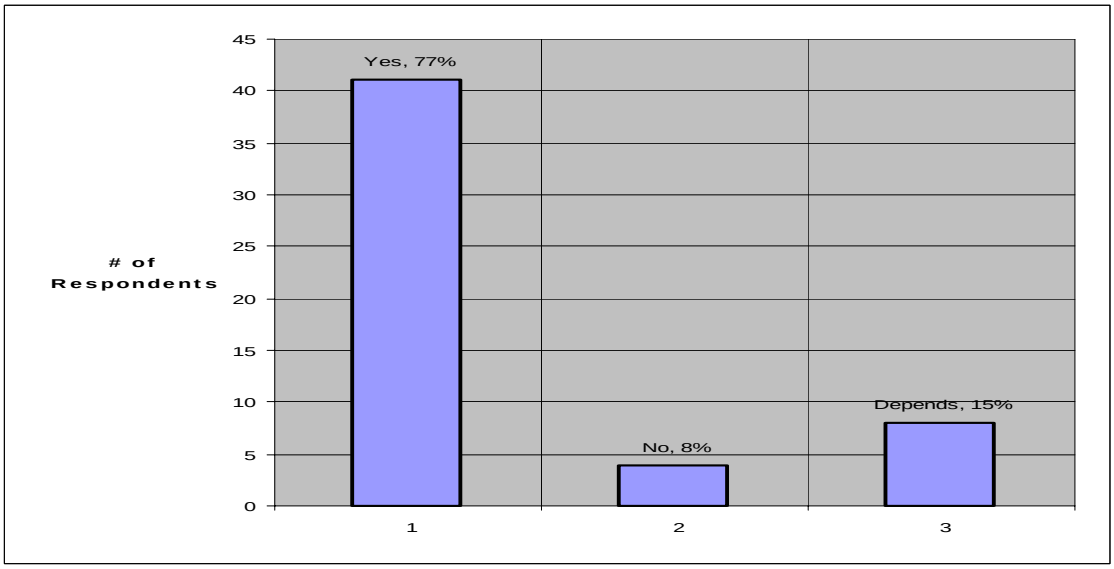



**Figure 14: Payback tour if certified at Government Expense.**

As shown in Figures 15 and Figure 16, there is a significant perceived value in industry IT certifications. This perceived value requires a commitment for the potential student. Certification is not a task to be taken lightly. This type of training requires intense preparation and study. The failure rate for an initial test is almost 50%. (Ashe, 2004)

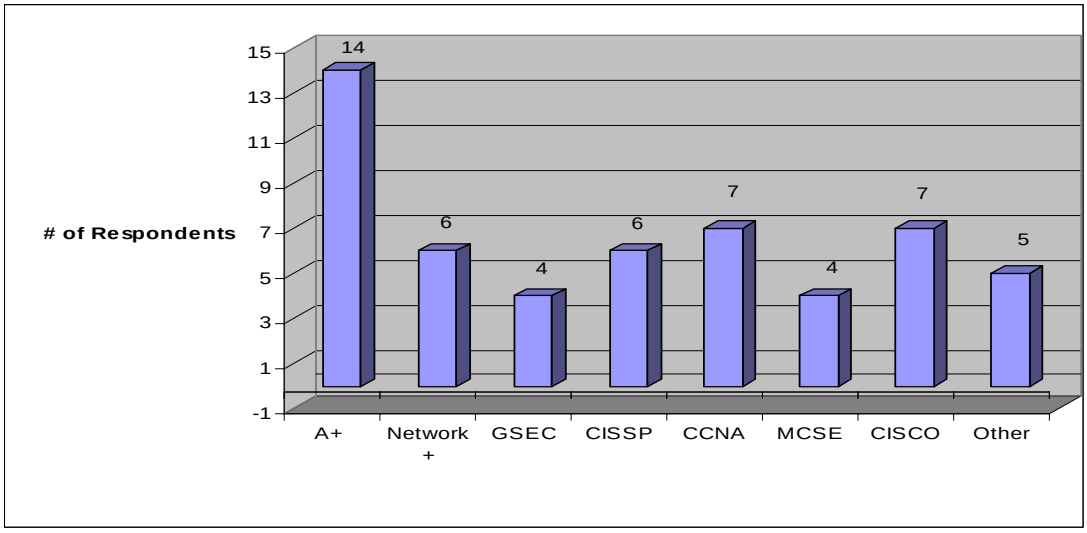



**Figure 15: Certifications Desired by Respondents**

Certification costs are prohibitive for the DoD. Unless Commanders are willing to pay for the certification training and testing, Marines will continue to progress in the current manner; to pay for the training and testing out of their own pocket.

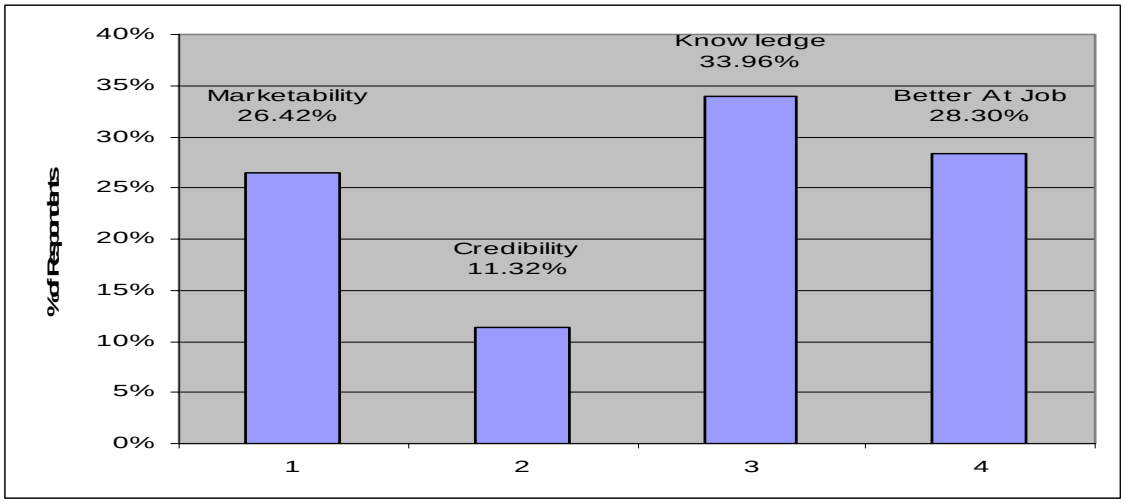



**Figure 16: Reasons for Certification**

### 4.4.3 Summary of Hypothesis 1

The null hypothesis stated that 50 % or more of System Administrator training is provided through formal schooling with the alternate hypothesis stating that less than 50 % of System Administrator training is provided through formal schooling.

Because the instruction method for System Administrator training is not consistent throughout the enterprise, Hypothesis 1 has examined how much of the required skill sets is attained through formal schooling.

Out of a total of 2470 responses, only 1372 responses were considered successes, or met the success threshold. Out of these 1372 responses, only 231 responses showed that they had received 50% or more of their training from MOS training. This 17% of successes is an indicator that System Administrators are not being trained to the standards that CJCSM 6510.01 has promulgated. Because of the small sample, inferences to the entire population of System Administrators are limited. The results of the survey clearly indicate a trend within the sample.

Investigative question 1 questions where the training of System Administrators is being conducted. The overwhelming majority is OJT at 40%. The second highest majority of training was received via self-taught method and MOS training finished 3rd with only 17%.

The problems with OJT were discussed with the main problem being the lack of consistency across the Marine Corps. Although OJT should not be considered a viable alternative to MOS school, OJT training that is provided after completion of MOS school will only reinforce and solidify the material taught in a formal environment. OJT training cannot arbitrarily take a back seat to MOS training though. OJT standards must be established and accomplishment monitored. Competent people must be selected and trained to conduct the OJT and required materials, equipment and time must be made available. (Tracey 1974)

Self-Taught method was the second majority method of training. It is out of the realm of this research to conduct a performance measurement on the effectiveness of self-taught material. It is important to note that because of the dynamic environment of the Marine Corps, the self-taught method easily lends itself to being available in many different situations, e.g. being able to study while in a deployed environment.

Investigative question 2 posits are private industry certifications an alternative method that can be used for DoD System Administrator certification?

The data indicates that while certifications are a universal objective among IT professionals, they are too cost prohibitive to the Marine Corps to be considered as an alternate method of certifying System Administrators.

77% of the Marine Corps System Administrators that responded to this survey said they were willing to re-enlist or extend their service obligation in return for certification training and examinations. Because of the commitment a potential student must agree too, re-enlistment or extension of service obligations are courses that the Marine Corps can take to attain a Return On their Investment. (ROI).

Currently Marine Corps Commanders will only pay for the certification examinations, not the actual training leading up to the examinations.

The caveat to this is that only Marines that are in the Occupational Field of 06XX are authorized to have their examinations paid for. This leaves other System Administrators in other OccFields to continue to pay for the training and examinations out of their own pocket.

### 4.5 Hypothesis 2 Analysis

Hypothesis 2 posits that there is no difference in the quality of training methods between formal schools and other training. The alternate to this is that there is a difference in the quality of training methods between formal schools and other training.

In order to test this hypothesis, a contingency table analysis was used. Contingency table analysis provides an instrument for analyzing possible relationships between nominal data with more than two outcomes.

Using contingency table analysis, the null hypothesis assumes that the two classifications are independent. The test for independence is conducted by comparing the actual cell count to the expected cell count.

Large values of $\chi^2$ indicate that the actual counts do not match the expected counts and the assumption of independence is likely false. Excel, (*Microsoft Excel*, 2002), is used in order to provide descriptive statistics about the data. The alpha in this research = 0.05. The method for executing a contingency table analysis is to first calculate the expected cell count, or the expected number of outcomes. The counts of the cells are used to determine dependency. This calculation was conducted by creating a pivot table in Microsoft Excel and placing the categories of training on the Y- axis and the quality, (1-5 likert scale) on the X axis. A pivot table was created for every question and an example is provided in Table 14.

**Table 15: Sample of Pivot Table used to calculate Cell Counts**

| Average of Q1QUALITY2 | QLTY | | | | | |
|---|---|---|---|---|---|---|
| Q1A | 1 | 2 | 3 | 4 | 5 | Means |
| 1 | 1 | 2 | 3 | 4 | 5 | 2.80 |
| 2 | 1 | 2 | 3 | 4 | 5 | 3.31 |
| 3 | | 2 | 3 | | | 2.50 |
| 4 | | | 3 | 4 | 5 | 4.00 |
| 5 | 1 | 2 | 3 | 4 | 5 | 3.29 |
| 6 | | | 3 | | | 3.00 |
| 7 | | 2 | 3 | 4 | 5 | 3.44 |
| Total | 1 | 2 | 3 | 4 | 5 | 3.22 |

After the pivot tables were created and filled, the data was summed and averaged to illustrate the cumulative average for the specific delivery method, which is depicted in Figure 17. Figure 17 also illustrates that there was not a significant difference in quality from one category to another. Certification quality was ranked the highest with an

average of 3.31. This would indicate that, while the certification training is costly, quality is an inherent part of the training.

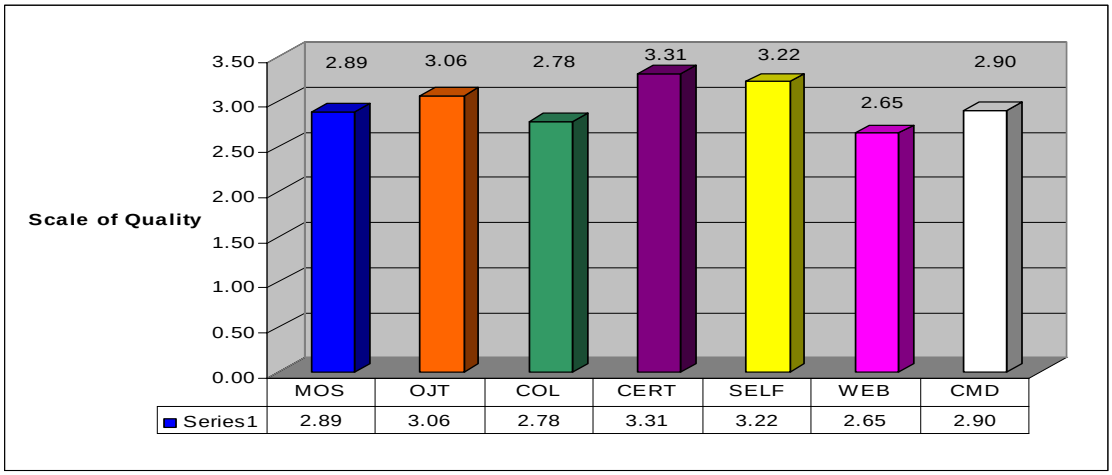



**Figure 17: Delivery Method Quality**

After the calculations were conducted in the pivot tables, the cell count totals for each category other then MOS, were summed as shown in Table 16.

Table 16 shows the observed values or cell counts for quality. These values were summed from each question and then totaled and added to the observed value table.

| Method of Training | | | 1 / Very Low | 2 / Low | 3 / Medium | 4 / High | 5 / Very High | SUM |
|---|---|---|---|---|---|---|---|---|
| | 1 | MOS | 63 | 105 | 149 | 100 | 40 | 457 |
| | 2 | Other | 200 | 244 | 673 | 451 | 175 | 1743 |
| | | | | | | | | 2200 |
| | | SUM | 263 | 349 | 822 | 551 | 215 | 2200 |

**Table 16: Observed Values for Quality of Training**

OJT received the highest number of cell counts but because this research has combined all of the other training delivery methods into the Other Category. Once the cell counts were completed, the expected cell frequency had to be calculated. This is

executed calculating Row Total * Column Total / N. N is the total possible outcomes which = 2200. For example: for the category MOS; 457 * 263 / 2200 gives you the expected value of the cell count. The expected cell count is illustrated in Table 17.

**Table 17: Expected Values**

| | | 1 / Very Low | 2 / Low | 3 / Medium | 4 / High | 5 / Very High | SUM |
|---|---|---|---|---|---|---|---|
| **Method of training** | MOS | 54.63 | 72.50 | 170.75 | 114.46 | 44.66 | 457.00 |
| | Other | 208.37 | 276.50 | 651.25 | 436.54 | 170.34 | 1743.00 |
| | | | | | | | |
| | SUM | 263 | 349 | 822 | 551 | 215 | 2200.00 |

After computing the expected values, the Chi-Square statistic is computed for each cell. Using a .05 level of significance with 4 degrees of freedom, the critical value of $\chi^2$ is 13.8484. The highlighted cells in Table 18 show that there significant differences in what the observed cell counts were from Table 16 and the expected cell counts from Table 17. Large values of $\chi^2$ indicate that the actual counts do not match the expected counts and the assumption of independence is likely false. The Chi-Square is calculated to be 26.4274. This indicates that there is a high dependency between the respondent's quality rating and the training received.

**Table 18: Chi-Square**

| | | | | | |
|---|---|---|---|---|---|
| MOS | 1.281639152 | 14.57245787 | 2.770931515 | 1.826228 | 0.486512484 |
| Other | 0.33603505 | 3.820776388 | 0.726515033 | 0.478822 | 0.127559498 |

| | | | |
|---|---|---|---|
| Chi-square | 26.42747636 | | |
| Degrees of Freedom | 4 | df = ( #Rows - 1 ) * ( #Columns -1) | |
| P Value = | 2.59451E-05 | P-Value Formula Check | 2.59451E-05 |

Table 18 illustrates the high dependency between how the training is delivered and the quality. For Hypothesis 1, the null hypothesis was rejected. As indicated in Table 18, the data indicates that the null hypothesis for Hypothesis 2 is also rejected because there is a strong indication of the dependency between the delivery method and the quality of training.

### 4.5.1 Summary of Hypothesis 2

For Hypothesis 2, the null hypothesis was rejected because the data indicates that there is a dependency between the delivery method and the quality of training. The data shows that the quality of training was the highest for certification training and lowest for web based training and college training. Based on a summated rating Likert scale of 1-5, the averaged responses ranged from 2.65 to 3.31. This indicates that there is not a large difference in the relative range of quality between the delivery methods. The data also supports that the quality of the training depends on the type of training received.

### 4.5.2 Summary

This chapter presented the results obtained during the study. Descriptive and binomial techniques were used to test hypotheses one, which was designed to analyze the where System Administrators are receiving their training.

The findings from the data analysis identify some significant findings relative to where System Administrators are receiving their training. Hypothesis 2 was tested using a contingency table analysis to test the dependency between the delivery methods of training, e.g. MOS school, compared to the quality of training. The data indicated that there is a dependency between the delivery methods used and the quality of training.

The following chapter will provide discussions, conclusions and recommendations based on the results presented in this chapter.

# V. Discussion, Conclusions, and Recommendations

## 5.1 Overview

The DoD, in an effort to establish benchmark training for System Administrators throughout the DoD enterprise, promulgated directives that established benchmark guidelines.

The overall purpose of this study was to examine if the Marine Corps's existing training meets requirements mandated by current DOD publications. Included in the research was an assessment of alternative training methods and the dependency between the quality of training and the delivery method.

This chapter presents discussions, conclusions, and recommendations for System Administrator Training, implications for the Marine Corps, limitations of the study, and recommendations for future research based on the analysis of the data.

## 5.2 Discussion and Conclusions of Hypothesis 1

The Chairman of the Joint Chiefs of Staff has mandated that all System Administrators, be certified and cleared to the level of information classification for a given system. The training must meet criteria set forth in the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01.

As discussed in Chapter 2, information technology is ubiquitous throughout the Marine Corps and System Administrators are the first line of defense against threats. They manage the day-to-day operations of the network and typically support 100 or more users. Respondents to this research survey show that a representative System Administrator is a 20-24 year old Marine with a rank of E-3 to E-5.

Although the data does not support that System Administrators are receiving 50% or more of their training at MOS school, the combination of MOS schooling and OJT is potentially meeting the criteria set forth in the CJCSM 6510.01.

Marine Corps formal schools that produce MOS Marines follow strict routines on the development of the curriculum. Twice a year, a panel of subject matter experts is invited to the school hose to conduct a Course Content Review Board, (CCRB) where each and every item within the curriculum is scrutinized for validity. Upon completion of the CCRB's, the new concepts are developed into a new curriculum.

All MOS training has been scrutinized for excess. Due to the operational tempo of the Marine Corps, it is mandated by HQMC that the pipeline from the recruiter to the unit be as short and quick as possible. This indicates that MOS training has been scaled down in an effort to increase the flow of Marines to their newly assigned units. While this type of "pipelining" has merit, the question becomes;" Is the gaining unit getting a Marine that has been trained to meet the expectations of the Commander?" This question is beyond the scope of this research effort but it points to further research. With the continuous deployment of Marines around the globe, Commanders may be content to have a warm body though they need a well-trained warm body. Operational commitments have priority over in-depth training which suggests that a young Marine needs to receive continuous training, via a locally-deemed method, until they have become proficient in their MOS.

System Administrators within the sample responded that they have received 17% of their training, at their MOS school. This would indicate that the standards set forth in the CJCSM are not being taught during MOS school. This is not an indicator that the

MOS school is inefficient. As stated previously, MOS schools are strictly governed by HQMC as to how long their curriculum can last. Given the constraints of these time limits, the training received at MOS school is more focused on Marine Corps policy and procedures and not local operations that are more detailed.

The overwhelming majority of responses indicated that OJT was the training method that was the most popular. The second highest majority of training was received via self-taught method. The self-taught method as shown in Figure 8 was the most popular method of preparing for a certification exam. 87% of the FBI / CSI survey responded that the self-study method was preferred. There are numerous methods to measure the effectiveness of the self-taught method. One means of measuring training is to conduct pre-training measurement, execute the training, give post-training measurement and then measure the change. (Craig 1976). This is a formal method of measuring performance while the self-taught method gives the impression to be less then formal.

The results of the survey imply that the self-taught method is a popular method of training among the respondents. Moore's Law states that technology doubles every 18 months, which necessitates the need to stay abreast of current technology. With MOS training and OJT training considered to be formal training, the self-taught method is the obvious means to stay current with the latest IT trends. Due to the continuing deployments of Marines, the self-taught method may be the only method of training that is readily available.

The last investigative question of Hypothesis 1 posits that private industry certifications could be an alternative method that can be used for DoD System

Administrator certification. The overwhelming response was that Marines were willing to extend their service obligations in order to attain certification. Data showed that this lust for the certification was not due to the want of more money, e.g. more marketable, but due to the quest for knowledge. HQMC is not willing to fund certification training for every System Administrator, but an alternative is to have Marines conduct the training. Several companies like Microsoft have courses that train the trainer. The concept is, once a person becomes certified in a certain area they can then become certified to teach their respective area. This program lends itself to Marines be able to train themselves without incurring the prohibitive costs and the formal certification classes and examinations for every System Administrator. The expense of the exam would still have to be funded by HQMC but the more costly training would be completed in-house.

### 5.3 Discussion and Conclusions of Hypothesis 2

The null hypothesis was rejected for Hypothesis 2, because the quality of training was dependent on the method of training. Because rating the quality is a perception of the respondents, this is a qualitative measurement that is subject to bias. (Phillips, 1983) This type of data is interpretative data. In order to validate the qualitative data, multiple sources of data are collected in the hope that they all converge to support the theory.

Conducting further research about the quality of training that system administrators receive will continue the learning cycle. Systems administrators are not only responsible for the efficient use of networks but also are the first line of defense against threats. By continuous learning and the validation of the training methods used,

system administrators can ensure that the quality of training they receive maintains an acceptable level.

### 5.4 Research Limitations

There are several limitations to this study that affected the overall outcome of the research. The Marine Corps' infrastructure is undergoing a complete overhaul with all of the garrison based IT assets being privatized under the NMCI contract. As the NMCI contract is being implemented across the Marine Corps, system administrators are being moved to different billets as needed with the training of the system administrators on the new system taking a low priority. In a recent Government Computer News, (GCN) NMCI survey, 42% of the respondents rated the training to be of poor quality on a scale of poor to excellent, (Walker, 2004).

While system administrators on the NMCI network are also required to be DoD certified, this is the responsibility of the primary contractor, Electronic Data Systems, (EDS). This flux of system administrator positions added an unknown as to the actual population of system administrators that the research survey would reach. Additionally, the survey response rate was less than 5% of the population which limits the inferences that can be made about the population.

The data collected was self-reported from system administrators across the Marine Corps. Self- reported data may include self-serving biases regarding personal work experiences, which may also have degraded the results.

Furthermore, this research is limited to the Marine Corps Population of System Administrators but the areas addressed in this research extend to not only all of the other

service components but also to all of the other federal agencies as well. Because this study was focused on the Marine Corps, it is not feasible in this work to generalize about System Administrators in the other components or agencies.

Next, the measures addressing the perceptions of the quality of training were not validated prior to the study. This type of validation is required because of the nature of the delivery methods. MOS training is very regimented with adherence to strict schedules being routine. OJT training is more relaxed, with the emphasis being on learning the day-to-day operations and less emphasis on training schedules and testing. This type of environment is more readily to be perceived as higher quality training than MOS training.

Furthermore, there were design flaws in the survey. When asked to rate the percentage of where they received their training for the two most influential categories for the particular question, the combined total of these two percentages should have only added up to 100%. This was not the case as respondents could mark 100% for both categories. Another flaw in the survey was that geographic location should have been more specific. The respondents were asked to mark what unit they were assigned to but not what base they were assigned to. This data would have been helpful in determining local trends. Additionally, there should have been a better explanation on where the actual questions were originating from, e.g., the DoD publication. This would have clarified the ambiguity of some of the questions.

## 5.5 Recommendations

The consequences of keeping System Administrator training stagnant or even slow to the technology changes will be the ill-prepared System Administrators manning the front lines of the network defenses. By using a Joint Task Analysis, (JTA) this will allow for the validation of the training and give a clearer picture of the required skill sets that have to be maintained in order to stay abreast with the technology and published mandates.

A JTA is a feasible construct that can be executed. JTA's are important as they provide important information about the job roles and tasks. These roles and tasks are judged important by the users, some of whom are experts in the end use of the products and in the services offered by the company. A JTA provides the basic information for evaluating the job skill and tasks, weighting them so the proper number of questions can be written for testing purposes.

The goal of a JTA is to create a description of the knowledge and skills involved in the successful performance at a job. A JTA is executed through a formal process where subject matter experts are gathered to address each of the following: a) the target audience for the training, b) the task and knowledge domains required for successful performance on each job role, c) the level of competence to be required for certification, d) gaps between target audience knowledge and skills and those required for certification, (Foster, 2000)

A JTA will provide a clear mechanism for the Marine Corps to access their current level of training for their system administrators and will clear the path for DoD certification for Marine Corps system administrators.

In order to comply with the DoD publications that mandate certification levels for System Administers, DoD agencies like the Defense Information Systems Agency (DISA) have the inherent responsibility to provide the means to the service components to attain the respective levels of DoD system administrator certification. This task is already being undertaken by DISA in the form of web-based and multi-media products that are available to commands to enhance the training. While these are quality training products, the end goal is to attain DoD certification for System Administrators.

In accordance with the Department of Navy Chief Information Officer, NMCI is currently making provisions to allow System Administrators to become certified which is another means to fulfill the DoD mandates.

### 5.6 Suggestions for Future Research

The Common Criteria Evaluation and Validation Scheme (CCEVS), is an activity jointly managed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The focus of the CCEVS is to establish a national program for conformance to the International Common Criteria for Information Technology. Through this body is the underlying acknowledgement that the training of users and System Administrators has to have some type of a benchmark in order to succeed.

Another area that can be researched further is a study into what the other service components are doing to accommodate the DoD mandates. This study focused on the Marine Corps, which is relatively small in numbers compared to the Army or the Air

Force. A study of System Administrator training for one of these components is likely to be a profound project with many complex issues.

## 5.7 Conclusions

The specific problem for this research effort was to determine if the Marine Corps's existing system administrator training meets requirements mandated by current DOD publications. Included in the research was an assessment of alternative training methods which could be used to meet the criteria set forth in the CJCSM 6510.01. Additionally, the quality of the existing training was assessed and found to be related.

Although inferences are limited, there are several indicators of where the training is being conducted and also the quality of the training. Based on the data shown in this research, System Administrators are receiving their training from a myriad of sources to include MOS, OJT and self-taught methods. The effectiveness of these methods has not been measured only that theses methods are the ones being used to deliver the material.

In the ongoing battle for control of the information space, System Administrators are the ground-troops and the first line of defense against attacks. In order to comply with the DoD publications that mandate certification levels for System Administers, the publishing DoD agency has the inherent responsibility to provide the means to the service components to attain the respective levels of DoD System Administrator certification.

# Appendix A: Skill Level 1 Training Requirements

| Knowledge | Skill | Ability | NIST Standard # 800-16 | NSTISSI #4013 |
|---|---|---|---|---|
| Formal training on the OS and command language or network protocols/operating parameters (network administration). | | Understand computer operating system fundamentals. | | |
| | | | | |
| Know rudimentary system/network administrator tasks relevant to the OS or network device. | | Understand and perform basic OS tasks. | 2.2C | |
| | | | | |
| Know OS, command language, and/or network protocols. | Manage system hardware and software. | | 2.2C | 1 b<br>2 c |
| | Manage accounts.<br>Maintain data store. | | | 2 d<br>5 c |
| | Provide communication connectivity and configure network protocols. | Install OSs, applications and peripherals; conduct testing and safeguards. | 3.3D<br>3.3E | 1 b<br>5 b |
| | | | | |
| Know normal operating parameters of relevant systems and applications. | | | 2.2C<br>3.3C | 1 a<br>1 b<br>2 c |
| Knowledge | Skill | Ability | NIST Standard | NSTISSI |

| | | | # 800-16 | # 4013 |
|---|---|---|---|---|
| Know basic system /configuration troubleshooting. | Troubleshoot problems. | Recognize abnormal operations. Recognize potential threats. | 3.1C<br>3.3C | 1 b |
| | Install and verify software patches. | Understand and perform basic system configuration and troubleshooting. | 3.5D | 1 b |
| | | Conduct informal, on-the-spot user assistance and training. | | 1 b<br>1 c |
| General knowledge of security features of operating systems and applications. | | Understand network security basics. | | 1 a |
| | | Understand the purpose of security devices (e.g., firewalls, host/network based intrusion detection systems, virtual private networks, and malicious code scanners. | 2.2D<br>3.1C<br>3.2B | 1 a<br>2 d<br>4 b<br>5 b |
| Knowledge | Skill | Ability | NIST Standard # 800-16 | NSTISSI # 4013 |
| | | Understand appropriate network and computer monitoring procedures. | 2.2D<br>3.1C<br>3.2B | 2 b |
| | | Understand the available mechanisms for detecting malicious code. | 2.2D<br>3.1C<br>3.2B | 5 b |
| | | Understand the definition | 2.2D | |

| | | | | |
|---|---|---|---|---|
| | | and purpose of cryptography. | 3.2B | |
| | Manage system security parameters | Able to configure system/network and application security parameters as required. | 3.4D<br>3.5D | 5 b<br>5 c<br>6 b |
| Formal training on IA awareness and common system/network vulnerabilities. | | Understand the evolution and principles of INFOSEC. | | 1 a |
| | | Understand and identify threats to information and information infrastructure. | 3.1C | 1 e |
| Knowledge | Skill | Ability | NIST Standard # 800-16 | NSTISSI # 4013 |
| | | Understand common vulnerabilities within an information infrastructure. | 3.4D<br>3.5D | 1 c |
| | | Understand the definition and characteristics of malicious code. | 3.4D<br>3.5D | 1 c |
| | Ensure security. Protect, detect, and react against system incursions. | Understand the principles of access level privileges (rings of protection/least privilege concept). | | 2 b<br>6 b |
| | | Assist IAO in access control security (passwords, auditing and alarming, etc.). | 2.1B | 4 b<br>4 c |
| | | | | |
| Know local IAVA procedures. | | Understand and react to | | 1 a |

| | | | | |
|---|---|---|---|---|
| | | vulnerability alerts (e.g., IAVAs). | | 1 b |
| Know local procedures for incident reporting and how to contact security assistance. | | Receive and initiate incident reports. | 1D | 1 b |
| | | | | |
| Basic knowledge of command/ organization's mission. | | | | 1 a |
| Knowledge | Skill | Ability | NIST Standard # 800-16 | NSTISSI # 4013 |
| Basic knowledge of command/ organization networks and systems. | | Understand network topologies. | 2.2C | 1 a |
| | | Understand internet working fundamentals. | 2.2C | 1 b |
| | | Understand the principles of risk management and risk mitigation. | 2.2C | 1 e |
| Know priorities for command/ organization networks and systems restoration | | Understand disaster recovery and continuity of operations concepts. | 2.2D | 5 a |
| | | Understand and perform system backup operations. | 3.5D | 6 a |
| | | Install emergency workarounds, as directed. | 3.5D | 5 b<br>5 c |
| Know about destruction plans and likely scenarios that trigger their execution. | Destruct ion techniques. | Assist with emergency destruction planning and execution. | 3.5D | 5 a<br>6 c |
| Knowledge | Skill | Ability | NIST | NSTISSI |

| | | | | |
|---|---|---|---|---|
| | | | Standard # 800-16 | # 4013 |
| Know basic differences between deployed (tactical) and garrison operating environments.* (agencies may want to focus on IA planning for rapid wartime/ contingency expansions. | LAN installation/repair. Network/system installation and repair. User assistance. | Able to operate in garrison and deployed environments, as required.* | 2.1B 2.1C | |
| | | | | |
| Know how to safeguard classified and sensitive data, both physical and electronic. | Maintain expertise. | Understand handling security procedures for classified/sensitive data. | 1D 1E | 1 b |
| | | Understand physical security principals. | | 1 a |
| | | Enforce physical and cyber-based security procedures. | 3.5D | 1 b |

# Appendix B: Research Survey

## A Study of Training Methods

The purpose of this survey is to measure attitudes toward the perceived value of training among System Administrators throughout the Marine Corps. This quantitative survey will be conducted on a two phase approach, web-based and mail-in. This survey will provide insight to what affects the perceptions of training has and what motivates future activities.

**Privacy Notice**

---

The following information is provided as required by the Privacy Act of 1974:

**Purpose:** To obtain information regarding training methods used for System Administrators.

**Routine Use:** The survey results will be used to provide developmental feedback for Training programs within the United States Marine Corps. A final report will be provided to participating organizations. No analysis of individual responses will be conducted and only members of the Air Force Institute of Technology research team will be permitted access to the raw data.

**Participation:** Participation is VOLUNTARY. No adverse action will be taken against any member who does not participate in this survey or who does not complete any part of the survey.

**Anonymity:** **ALL ANSWERS ARE STRICTLY ANONYMOUS.** Thus, your name will not be included anywhere on this questionnaire.

---

**INSTRUCTIONS**

- Base your answers on your own thoughts & experiences
- Please print your answers clearly when providing comments
- Make dark marks when asked to use specific response options (feel free to use an ink pen)
- Avoid stray marks and if you make corrections erase marks completely or clearly indicate the errant response if you use an ink pen

**MARKING EXAMPLES**

| Right | Wrong |
|---|---|
| ● | ⊗ ⊘ ⊙ |

**ALL RESPONSES/COMMENTS DIRECT TO:**

GySgt B.K. Hamilton
AFIT/ENV 04, BLDG 640
2950 Hobson Way
Wright-Patterson AFB, OH 45433-7765
Email: brian.hamilton@afit.edu
Phone: DSN 785-3636, Commercial (937) 255-3636
Fax: DSN 986-4699, Commercial (937) 656-4699

**SECTION II**
**BACKGROUND INFORMATION**

**This section contains items regarding your personal characteristics. These items are very important for statistical purposes. Respond to each item by WRITING IN THE INFORMATION requested or CHECKING THE BOX ☑ that best describes you.**

1. MOS:

0651 0653 0656 0658 0659 0681 0689 06XX 01XX 30XX Other pls specify_____

2. What Unit are you presently attached to?

MCB 1stFSSG 2dFSSG 3dFSSG 1MARDIV 2MARDIV 3MARDIV

1MAW 2MAW 3MAW MEU/MEB Other pls specify_____

3. Rank / PayGrade(Civilian)

4. What are your primary job responsibilities?

System Administrator HelpDesk Technician Technical Support Database Administrator

Network/Gateway Administrator to include e-mail, firewall & IDS Web Site Administrator

Operations Security / Physical Security Security Administrator (EKMS) DMS System Specialist

Other…please explain

5. How long have you been working with computers/networks in the Marine Corps?

1-3 yrs 4-6 yrs 7-9 yrs 10 yrs and above

6. Environment

How many users do you have? How many servers do you own? How many different applications do you have on your systems?

How many domains do you administer? How many people do you have working for you?

7. What certifications to you currently have?

A+ Network+ CISSP GSEC MSCE CISCO CCNA other?

8. What certification would you like to attain?

A+ Network+ CISSP GSEC MSCE CISCO CCNA other?

9. Payback Tour
Would you be willing to do a 1 yr payback tour if the Marine Corps paid for you to go thru certification training and take the test??

Yes No Maybe…specify_____

10. Why do you want to become certified? (pick only one)

More Marketable on the outside Increase credibility Increase knowledge Test Ability

Get a different job w/I Marines To be better at your job

11. Please indicate highest level of education that you have attained.
Some HS
HS Diploma
Assoc Degree
Bachelors Degree
Master's Degree
PhD
Other

12. What is your age____Yrs

**This section asks questions concerning where you received your training. Although it is recognized that a majority of your training is a combination of the categories, it is requested that you only mark TWO categories for each question, whichever 2 categories had the greatest percentage of your learning the area in question.**

**SAMPLE**

**Each question requires 3 items: Identify % of training, Where you received training, and Quality of training.**

| | ① MOS School | ② OJT | ③ Local Comm. College | ④ Certification Training | ⑤ Self-Taught | ⑥ Distance Education/MCI/ Web-based | ⑦ Local Cmd training | Quality of Training 1-5 |
|---|---|---|---|---|---|---|---|---|
| 1. Recognize potential security violation & take appropriate action to report incident and stop/fix any adverse impact. | %___55_____ | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| | %___45_____ | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |

**The above question shows that this Marine received 55% of his training for this question at MOS School w/ the quality of the training being rated 3. The Marine also received 45% of his training from OJT w/ the quality being 2.**

| | ① MOS School | ② OJT | ③ Local Comm. College | ④ Certification Training | ⑤ Self-Taught | ⑥ Distance Education/MCI/ Web-based | ⑦ Local Cmd training | Quality of Training |
|---|---|---|---|---|---|---|---|---|
| 1. Recognize potential security violation & take appropriate action to report incident and stop/fix any adverse impact. *Cell 1D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 2. Understand physical security principals. *Cell 1D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 3. Understand security procedures for handling classified/sensitive data. *Cell 1E* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 4. Identify laws & regs applicable to specific info systems or applications (e.g., ATLASS II, UMIPS, Unit Diary). *Cell 1E* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 5. Advise on security requirements for new IT purchases. *Cell 2.1B/3.2B* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 6. Assist in access control security (e.g. passwords). *Cell 2.1B* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 7. Know basic differences between deployed and garrison operating environments. *Cell 2.1B/2.1C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 8. Advise on a IT security program/plan for your unit. *Cell 2.1C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 9. Understand categories of risk and help design IT security procedures for your unit. *Cell 2.2C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 10. Understand disaster recovery and continuity of operations. *Cell 2.2D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 11. Apply specific IT security procedures and ID areas of weakness. *Cell 2.2D/3.1C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 12. Understand the purpose of security devices (e.g., firewalls, IDS's, VPN's,) *Cell 2.2D/3.1C/3.2B* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 13. Understand the definition and purpose of cryptography. *Cell 2.2D/3.2B* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 14. Install and operate IT systems in a test configuration that do not alter the program code or compromise security safeguards. *Cell 3.2D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 15. Design and develop tests for security safeguard performance under normal conditions/operating circumstances. (e.g. test for open ports) *Cell 3.3C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 16. Conduct tests of security safeguards iaw the established plans and procedures. *Cell 3.3D/E* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 17. Install OS's, applications and peripherals. *Cell 3.3D/E* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 18. Identify IT security impacts upon implementing a new OS or application. *Cell 3.4C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 19. Implement safeguards for an IT system iaw established plan. *Cell 3.4D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 20. Understand security procedures & the assignment of responsibilities to ensure personnel are complying with them. *Cell 3.5A* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 21. Design/develop new IT security procedures in response to new operating environment. *Cell 3.5C* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |
| 22. Monitor system activity to ID potential IT security events. *Cell 3.5D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① ② ③ ④ ⑤ |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 23. When system is being DRMO'ed, ensure all security concerns have been addressed, (e.g., Hard drives wiped iaw DoD regs). *Cell 3.5D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① | ② | ③ | ④ | ⑤ |
| 24. Understand and perform system backup operations *Cell 3.5D* | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① | ② | ③ | ④ | ⑤ |
| 25 Understand Internet working fundamentals. | ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ① | ② | ③ | ④ | ⑤ |

## Bibliography


Agresti, A. *An Introduction to Categorical Data Analysis.* New York: John Wiley & Sons, 1996

Ashe, J.A. "Certification: At What Cost," ComputerWorld, v32, No 04, March 2000

Bellocci, T., et al., "Information Assurance in Networked Enterprises: Definition, Requirements and Lab Experiments", CERIAS Technical Report 2001-34, Retrieved 25 \
June, 2003, from http:// www.gilbreth.ecn.purdue.edu/~prism/publications.html

Brenner Susan, *Definition of Social Engineering* University of Dayton School of Law, Dayton OH, 2001

Computer Security Institute / Federal Bureau of Investigation, *Computer Crime and Security Survey*, San Francisco CA, March 2003

de Zafra Dorothea, "The Human Factor in Training Strategies," a presentation to the Federal Computer Security Program Managers' Forum, November, 1991.

Department of Defense. *Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND).* CJCSM 6510.01, Washington: Pentagon, March 2003

Department of Defense. *Information Assurance (IA) Implementation* DODI 8500.2, Washington: Pentagon, February 2003

Department of Defense. *NSTISSI Number 4009, National Information Systems Security (INFOSEC) Glossary*, Washington DC, November 2001

Department of Defense Chief Information Officer, (CIO) *Joint Vision 2020*, Washington: Pentagon, February 2003

Defense Information Systems Agency. *Defense in Depth* Version 1.0 (CDROM). August 2001

Department of Labor, Bureau of Labor Statistics. Retrieved 12 June, 2003, from http:// www.bls.gov/oco/ocos268.htm

Dulany, Kevin M. "Information Assurance Update," a presentation to Information Assurance Conference, Williamsburg, VA. 2003

Federal CIO Council, Federal Conceptual Model Subgroup. (1998) *Federal Enterprise Architecture Conceptual Framework*. Retrieved 17 Jul, 2003, from https:// www.cio.gov/Documents/fedarch1.pdf

Foster D. et al. *The Importance of Job Task Analyses.* Retrieved 13 January 2004 from http://www.computer.org/certification/procert_jta.html

Gay, L.R. *Educational research: Competencies for analysis and application.* 5th Edition. Upper Saddle River NJ: Merrill/Prentice Hall. 1996.

Hrebec G. *Network Administrators: Knowledge Management*. SANS Institute Online Retrieved 1 Aug, 2003, from http://www.sans.org

International Information Systems Security Certification Consortium, Inc. Retrieved 22 August, 2003, from http://www.isc2.org

Johns Alan. *Certification Blues*. Retrieved 1 Aug 2003, from http://www.cert.org

Lemen Amy E. *Certification Industry Revenues*. Retrieved 23 Jan 2004, from http:// www.business.com

Maconachy W. V. *Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation into 1 Practical Reality,* Proceedings of the 12 National Computer Security Conference, October 1988.

Maconachy et al. *INFOSEC Professionalization: A Road to be Traveled,* Forum for Advancing Software Engineering Education, v 9, No. 01, January 1999

McClave et al. *Statistics for Business and Economics*, 8th Edition, Upper Saddle River NJ: Merrill/Prentice Hall. 1996.

Neacy et al. *Resident Perception of Academic Skills Training and Impact.* Retrieved 15 January 2004 from http:// www.saem.org

NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role-and Performance-Based Model*, April 1998

OASDC3I, *Improving Information Assurance: A general assessment and Comprehensive Approach to an integrated IA Program for the Dept of Defense*. March 1997

Oser, R.L., *Emerging themes in distance learning research and practice*. Retrieved 12 January 2004 from http:// www.hf.faa.gov.

PCIPB Memorandum. *Establishment of Board Standing Committee on Education.* Washington DC. March 2002

Sage Salary Survey. Retrieved 18 Aug, 2003, from http:// www.usenix.org/sage/jobs/salary_survey/salary_survey.html

SANS Institute Online, *A Cooperative Education and Research Organization*. Retrieved 12 Jul, 2003, from http://www.sans.org

Smith K. *Security Awareness: Help the Users Understand*. SANS Institute Online Retrieved 12 Jul, 2003, from http://www.sans.org

Thomas Bellocci et al. "Information Assurance in Networked Enterprises: Definition, Requirements, and Experimental Results" *CERIAS, TR 2001-34 School of Industrial Engineering,* No. 01-05 (January 2001)

Thompson Prometric, *New Study Guides for Certification*. Retrieved 10 October 2003 from http://www.prometric.com/itstudy2001/

Tittel, Ed. *The Cost of Certification*, Certification Magazine, February 2004.

Tracey, William R. *Managing Training and Development Systems*, American Management Associations, New York, 1974

Walker, Richard W. *....as Navy users sound off on problems.* Government Computer News, volume 23, number 4, February 23, 2004. Washington, DC

Worthen, Ben. *Measuring the ROI of training*. Retrieved 15 January 2004 from http://www.itworld.com/Man/2818/CIOroi.html

## Vita

GySgt Hamilton enlisted in the Marine Corps in October 1981. He began his career in Okinawa, Japan, with Headquarters Company, 9th Marine Regiment in April 1982, serving as a Supply Clerk. In May of 1983, he was ordered to New River Air Station, North Carolina where he served with Marine Aircraft Group 29, for 3 years. In August 1985, he reported to Quantico, Virginia for duty as a Marine Security Guard.

From September 1987 to October 1991, GySgt Hamilton was assigned to Amphibious Warfare School where he was served as a Logistics Non-Commissioned Officer, (NCO). After completing his tour at Quantico, GySgt Hamilton returned to Japan where he was assigned to 3rd Supply Battalion, 3rd Force Service Support Group. From November 1991 to November 1994, GySgt Hamilton served as a Network Administrator and as a Supply Analyst.

In January 1995 to July 1998, GySgt Hamilton was assigned to Inspector-Instructor Duty, Madison, Wisconsin where he served as a Supply Chief in support of Gulf Company, 2nd Battalion, 24th Marines.

From August 1998 to August 2000, GySgt Hamilton was assigned to Supply School, Marine Corps Combat Service School, Camp Johnson, North Carolina, where he served as an Advanced Logistic Instructor, and as the Network Administrator.

In August of 2002, GySgt Hamilton entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be retiring from the Marine Corps.

# REPORT DOCUMENTATION PAGE

*Form Approved OMB No. 074-0188*



**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From – To)* |
|---|---|---|
| 23-03-2004 | **Master's Thesis** | Aug 2002 – Mar 2004 |

**4. TITLE AND SUBTITLE**

EMPOWERING MARINE CORPS SYSTEM ADMINISTRATORS: TAXONOMY OF TRAINING

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Hamilton, Brian, K., Gunnery Sergeant, USMC

**5d. PROJECT NUMBER**
If funded, enter ENR #

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)**

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB OH 45433-7765

**8. PERFORMING ORGANIZATION REPORT NUMBER**

AFIT/GIR/ENV/04M-09

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

HQMC / C4
Attn: Mr Letteer
LFF-1
2 Navy Annex,
Washington, DC 20380-1775.

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

Organizations cannot protect the integrity, confidentiality, and availability of information in today's highly networked systems environment without ensuring that System Administrators are properly trained and meet a minimum standard that is enforced enterprise-wide. Only with this ubiquitous benchmark training, will the System Administrators roles and responsibilities become synchronous to achieving Defense in Depth in the IT realm. The goal of this research is to analyze Marine Corps training methods to identify viable solutions that will produce consistent skill sets and that meet requirements set forth in mandates from DoD.

**15. SUBJECT TERMS**

Information Assurance, security, information warfare, knowledge management, education, training, measurement, quality, contingency table analysis.

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **REPORT** | **ABSTRACT** | **c. THIS PAGE** | | | Alan R. Heminger, PhD |
| **U** | **U** | **U** | **UU** | 106 | **19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4797; e-mail: Alan.Heminger@afit.edu |